[illegible]

[illegible]

Reproduction of this document or any part thereof is forbidden without the express approval of the Executive Officer, Science Advisory Committee to the President.

SCIENTIFIC JUDGMENTS

ON

FOREIGN COMMUNICATIONS INTELLIGENCE

Special Intelligence Panel
of the
Science Advisory Committee to the President
The White House, Washington, D. C.

23 January 1958

Copy No. 4 of five copies.
This document consists of 167 pages.
Series A.

The principal findings and judgements of the study are condensed in the following 4-page Digest.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[illegible]

Scientific progress has gravely modified our capabilities in communications intelligence (COMINT). During World War II, cryptanalysis supported by information from [redacted] sources about enemy techniques gave us immediate and complete access to most enemy high-level communications. COMINT is still of great value. [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Only further research will disclose the possibility and extent of exploitability. Even with the greatest optimism, it is clear that [redacted] Our cryptanalysts believe that some of our own cipher machines are entirely unreadable with foreseeable technology, even if the enemy has a complete machine, and we have no reason to feel that a similar degree of security is beyond the capabilities of other countries.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Advances in the science and technology of cryptology tend to increase the effectiveness of cipher machines more rapidly than they increase our ability to read such machines. This accounts for our [redacted] Indeed, it is only through the extraordinary ingenuity and skill of our cryptanalysts that we are able to [redacted] and [redacted] as we do.

Only through research on the fundamental problems of cryptology, as well as [redacted] themselves, can we hope to deal with the increasing effectiveness of the cipher machines of [redacted], and perhaps to read messages that are now undecipherable. The cryptanalyst needs maximum assistance from [redacted] action undertaken to discover both how enemy cipher machines are constructed and how they are used. Modern cryptographic systems include elaborate safeguards to limit one's losses in the event the system is breached. We must assume that in many cases success, by whatever method, may mean the ability to read either a small group of messages or a continuing small sample of messages, rather than the complete traffic.

Signals can be most effectively exploited by integrating the processing of COMINT and ELINT and by speeding and improving collection and processing. This calls for certain organizational and technological changes, and for strong and effective leadership by the NSA.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Our chief recommendations are:

(1) Vigorous and expanded prosecution of cryptanalytic research is required, in order both that we may continue to [redacted] We recommend establishing a contract-managed research institution on the pattern of Los Alamos. It should combine NSA's present cryptanalytic and mathematical research people, the best groups now working on [redacted] and others.

(2) The over-riding priority assigned to the reading of [redacted] should be relaxed. The intellectual problem is much too refractory to yield to administrative pressure, and extreme emphasis on this one project hampers the NSA and belittles its many valuable contributions in other directions.

(3) The non-research components of NSA should be judged solely on the basis of the timely production, and efficient supply to consumers, of intelligence derived from all directly exploitable communications and electronic intercepts. To this end a much more vigorous program of systems engineering is required. The development program, now conducted in NSA's R/D, will require strengthening and expansion.

(4) To this end also, we recommend the responsibility for and control of ELINT processing and analysis be assigned to the National Security Agency.

(5) Collection of signals accounts for three-fourths of the cost of communications intelligence operations. Efficiency requires (i) a complete engineering and organizational overhaul of collection and field processing operations, (ii) transfer of field processing activities to the NSA, (iii) a careful technical scrutiny of what and how much is collected and of possible duplication of facilities by the various services. Modification and consolidation of field operations offer the greatest opportunity for increased efficiency in communications intelligence.

(6) Increased emphasis should be placed on [redacted] contributions to the COMINT problem.

(7) The NSA should be given full authority to exercise vigorous and effective leadership at all levels in communication intelligence operations, especially in the day-to-day operation of collection and processing activities.

Our intelligence program is a major technical weapon. COMINT and ELINT are vital for us in our struggle with a capable and secretive adversary.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

SYNOPSIS

The Panel assembled by the Science Advisory Committee of the Office of Defense Mobilization, at the direction of the President, has studied the derivation of foreign intelligence, particularly from the most secure coded communications of the [redacted] It was early apparent that some other methods of gaining foreign intelligence should be included in the study, and, after appropriate consultations, the charge to the Panel was somewhat broadened. The work of the Panel has been chiefly based on information obtained from the NSA, as the principal organ of foreign communications intelligence, but the cooperation of several other government agencies is acknowledged.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The Panel has been impressed by the complexity of the cryptanalytic problem, and the variety of military, political, and technological considerations which enter into the over-all situation. It has been particularly impressed by vast changes which recent years have brought. Among these are

(1) A great increase in the relative importance of COMINT activities due to the fact that the [redacted] has substantially shut off so many usual open and [redacted] sources of intelligence. This has led to a great increase in the bulk of intercepted COMINT material compared with any previous peace-time period.

(2) The great increase in the importance and urgency of certain kinds of COMINT intelligence because of the great speed and destructive power of modern weapons.

(3) An improvement in the understanding and technology of cryptography which has led to the wide use of cipher machines which have proved invulnerable even when attacked with the aid of the rapidly advancing art of electronic computation.

The magnitude of these changes is so great that the role of COMINT in our intelligence effort cannot be properly judged on the basis of previous experience. Intelligence plans and actions need to be thought through from the beginning. The Panel has made no attempt to undertake such a complete review. It has, however, emerged with a number of conclusions, which it feels must underlie any general reconsideration. Its conclusions and recommendations are expressed in detail in the various sections of the report, which are summarized below.

I. Introduction

Much of the judgment of the Panel concerning the intelligence problem relates to the best utilization of our national technical abilities. Because these are concentrated in the NSA, the structure and operations of the agency are subjected to searching scrutiny. Recommendations for changes should not be construed as a criticism of that highly competent agency in its present role, but rather as indications as to how it could be redirected to best contribute to the over-all intelligence problem.

II. [redacted]

No national strategy should be based on the hope or expectation that we will be able to read [redacted] of less than the highest level are enciphered by a machine called [redacted] has not been read and the Panel believes current and useful reading in peace time is unlikely by cryptanalysis unaided by [redacted] activity. An increasing amount of both [redacted] is routinely [redacted] The Panel believes that this also will never be read completely although a small part, not of our choice, may or may not be read because of errors in operation. The prospect of our being able to read messages [redacted] first by [redacted] something which would for the [redacted] be technically straightforward and would presumably be done routinely (and apparently has begun) when unusual security is desired, is of course smaller yet. Technology is irresistibly making the situation worse rather than better, and what is now true of the [redacted] may become true of other, technically less-sophisticated countries.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

We should nevertheless continue the most vigorous attack on [redacted] Only thus can we possibly hope to exploit any errors which may occur in times of emergency; only thus can we hope to sharpen our cryptanalytic weapons against the increasing sophistication of [redacted]

There is no limit to the potentialities of [redacted] activity. If machine plans, key usage schedules, and operational information are stolen, any system can be read. Information on the construction of such a machine as [redacted] (without extensive key information) might not lead to reading the machine, but it could be equivalent to many years of cryptanalytic work.

(b)(3)-P.L. 86-36

It appears that we must revise our view of communications intelligence activities. In the foreseeable future we must develop a philosophy of fragments, in which rare and isolated readings [redacted] will be a small if vital addition to information derived from irregular reading of not quite [redacted] and from a great mass of [redacted] sources.

III. Collection of Intelligence Signals

The world-wide interception of signals is the costliest part of COMINT activities. The volume of intercept is out of proportion to the value of its content or to the practical possibility of subjecting all of it to even a minimum of cryptanalytic scrutiny. Completeness of intercept and exploitation is impossible, and we must make the wisest sampling of [redacted] traffic. Some traffic, such as that [redacted] and [redacted] may have to be intercepted as fully and processed as speedily as possible. Other traffic may be sampled. An effort should be made to identify [redacted] in the field so that related, potentially exploitable, traffic may receive priority of interception and transmission. A thorough-going reorganization and mechanization of collecting activities is called for.

The tremendous volume of [redacted] communications intercept and the great range of other important radiations call for integration of collection and identification activities. Changes in communication signals and the use in some [redacted] communications of increasingly high frequencies, including the [redacted] range, have made communications signals hard to distinguish from [redacted] radiations. Duplication and separate operation of intercept facilities, and separate processing, such as in operation at Kelly Field, are not only costly; they could lead to dangerous delays in the interception and evaluation, and even the identification, of new signals. An incomplete evaluation of signals through separate intercept and processing of various radiations might lead to tragic mistakes or oversights in an emergency.

All ELINT processing and analysis activities should be unified with COMINT activities under the direct control of the NSA, whose wide scope and unparalleled technical competence afford the proper setting for this essential integration of effort.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

A new sense of urgency and a new emphasis on speed of processing must be developed at the NSA in connection with the handling of vital [redacted] material, such as that concerned with [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

A collection and processing exercise is recommended in order to evaluate the speed with which the NSA could intercept, process and make available intelligence information under simulated emergency conditions.

IV. <u>Processing and Analysis of Communications Intelligence</u>

In order to cope efficiently and promptly with the tremendous bluk of COMINT material of all levels, great advances must be made in the use of machines both in the preparation of material and in cryptanalysis itself. This requires, among other things, that material be recorded in the field in a manner suitable for machine reading, or for swift, automatic communication to machine headquarters.

A vigorous, independent, and well-directed program of systems engineering and development is called for, both in the specific area of machine-readable recording at intercept and in the general area of machine processing and [redacted] Many suggestions in this direction have already been advanced.

V. <u>Foreign Intelligence Sources Supplementary to</u> [redacted]

COMINT objectives should realistically reflect the accessibility as well as the potential value of material.

Presumably, the information contents of many secret messages are actually reflected in masses of accessible communications. A careful study of the relations between the content of [redacted] communications, extending beyond mere traffic analysis, should be made for some period in the past during which both were available.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The utmost attention should be given to [redacted] materials during periods which may prove unusually rewarding because of such internal changes as the industrial change which [redacted] is now undergoing.

It will be profitable to cultivate assiduously not only [redacted] countries, at least in connection with [redacted]

VI. NSA--The National Resource for Communications Intelligence

Past wartime successes in reading the [redacted] communications have established an ideal image, a standard, a set of values in the NSA which is reflected in its organization and operations, but which is not appropriate to the realities of today. What is needed now is a complete division between cryptanalytic research on [redacted] and the actual production of current intelligence.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Unless the work on [redacted] is not only maintained but strengthened, we will throw away not only the remote chance of [redacted] in the future, but also any possibility of [redacted] traffic [redacted] for the encipherment of such traffic is bound to become more and more effective.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Cryptanalytic research could best be strengthened by establishing a contract-managed research institution on the pattern of Los Alamos, including NSA's present cryptanalytic and mathematical research people together with the best of the groups now working in PROD on [redacted] The personnel of this institution should be fully cleared and informed of NSA activities, and should both conduct basic cryptanalytic research and attack [redacted], to the point of, but not beyond "production" exploitation. The successful operation of such an institute calls for the ultimate in effort and selection in the recruiting of personnel.

P

The remainder of the NSA should have as its enthusiastic aim the most rapid and skillful supply of communications intelligence to users, based on currently exploitable COMINT material and on ELINT material. It should be supported by a vigorous systems engineering and development program directed at the over-all problems of improvement and mechanization of the collecting and handling of material.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

In order to secure the most from [redacted] operations and to make the best use in them of the technical knowledge and strength of the NSA, much more detailed technical cooperation should be promoted between the NSA and the CIA.

A small group concerned with intelligence <u>about</u> cryptology should be established somewhere in the U. S. intelligence community.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

TABLE OF CONTENTS

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

OGA

TOP SECRET EIDER

SCIENTIFIC JUDGMENTS ON FOREIGN COMMUNICATIONS INTELLIGENCE

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

PREFACE

The Panel assembled by the Science Advisory Committee of the Office of Defense Mobilization, at the direction of the President, has studied the derivation of foreign intelligence, particularly from the most secure coded communications of the [redacted] The facts faced suggested that certain aspects of other forms of gaining foreign intelligence should also be studied. The charge to the Panel was then, following consultation with appropriate individuals, correspondingly broadened.

Concern with the results of this study is associated with differing interests, responsibilities, and activities. Accordingly, the report has several aims, prominent among which are:

(1) Offering of judgments about exploiting the most difficult [redacted] in order to provide a scientific basis for policy decisions.

(2) Surveying possible advances in the technology of exploiting [redacted] in order to ensure consideration of the application of all presently conceivable facilities to the problem.

(3) Proposing a revised evaluation of foreign communications intelligence, in order to develop a more quantitative basis for the most appropriate distribution of technical effort.

(4) Exploring the technical advantages of further coordination of the signal intelligence community, including the relation of ELINT activity to COMINT.

(5) Recommending some altered features of National Security Agency's structure and operation, in order that the Agency may meet the present and future challenges of foreign communications sources particularly well.

(6) Providing an open view of the basic issues of communications intelligence and cryptanalysis in terms of modern science, in which the future problems of decipherment, processing, and interception are outlined in generalized aspects.

These objectives relate to the administrative, military, diplomatic, technological, and professional aspects of the intelligence community. Because of this diversity, several levels of technical detail are included in the report. The appendices provide detailed support for the conclusions stated in the body of the report. The technical adjuncts cover more technical aspects of specific situations.

The body of the report begins with an introductory section which attempts to place the exploitation of [redacted] communications in the hierarchy of our technological national security effort. The work on the [redacted] is summarized in the second section, in order to bring out the present position in [redacted] ciphers. The third section covers the original sources or interception of our whole communications take. This lays a basis for consideration of the total raw material available to supply the changing intelligence needs. Methods of handling the total collection we may be able to acquire are treated in the fourth section, which deals in particular with processing and analysis preliminary to reading or other disposition. The fifth section treats the changing position, in foreign communications intelligence, of [redacted] ciphers. In this connection, [redacted] Finally, recommended modifications on the form and operation of the major communications intelligence instrument, the NSA, are discussed in the sixth section.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

I. INTRODUCTION

In the continuing cold-war struggle, encrypted material presumably contains vital information concerning intentions and plans of the adversary: what bluffs will be sustained, what forces will be readied, what weapons prepared. The use of enciphered material together with the [redacted] acquisition of documents and intelligence is a battle in which we and our allies can gain or lose substantially. As Communism centers around the control of the mind and spirit, so one of its strongest weapons is the control of information.

Unfortunately, in peace time, if not in war, enciphered communication can be used deliberately and with care, so that today the sorts of errors which lead to war time successes seldom occur. In peace it is also very much harder to associate communications with the sort of observable events which might give a clue to their contents.

The National Security Agency has wisely been created to deal with this very difficult situation. This Panel sees the NSA as the principal force in our struggle for such information.

The Panel believes that if we are to gain crucial knowledge of the weaponry, capability, and intentions of foreign countries, the signal intelligence community must be a unified organization. [redacted] have encompassed the vast bulk of the [redacted] communications whose significance will be discussed in the following sections. To deal with this situation with any effectiveness, our communications intelligence skills, particularly our cryptanalytic skills, must be completely integrated. Dispersion can lead only to the scattering of our meager decipherment talents and to an ineffective and inefficient use of them.

√β

Accordingly, much of the judgment of the Panel on the foreign intelligence problem will relate to the utilization of our national technical abilities. Because these are, fortunately, now mostly concentrated in the NSA, the structure and operations of the NSA will be subjected to searching scrutiny.

This should not be construed as a criticism or evaluation of the Agency in its present role, but rather as an inquiry into how it could best contribute to the overall foreign intelligence problem. At the outset we render to the NSA the highest confidence and admiration that we know. Its technical achievements are unexcelled, and it deserves the unqualified confidence and support of all civilian and military departments and agencies.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

II. [redacted]

It must now be said that it is not likely that [redacted] soon be read, and that some of these cannot possible be read, except through the grossest misuse or through the [redacted] acquisition of supplementary information. So-called pad systems are an example of this last, most difficult situation.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

In a pad system each character of a message is enciphered with a corresponding character of key material. The used key material (another copy of which is necessary for the decipherment of the message) is then destroyed. If the key material is properly produced, as [redacted] key now almost certainly is, and if the key is used but once, as [redacted] key now almost certainly is, such encipherment is, both theoretically and practically, <u>completely unreadable</u>, and this fact has long been recognized.*

---

* This paragraph summarizes one area of the subject called <u>cryptology</u>. In it, the cryptographer devises either intricate key material or machines for transforming the successive characters,

or groups of characters, of the message in intricately changing ways. When a key is applied to a message, its language and meaning are hidden but it still remains in a form which is convenient to communicate accurately. The cryptanalyst tries to unravel these keys or machines in order to learn the meaning of the signals transmitted. One-time use of random key, in spite of the fact that it makes a message completely unreadable, since nothing can be deduced about any one character from a knowledge of all the other characters of the same key, is not convenient and becomes cumbersome when the volume of messages to be communicated is large. Therefore, other ways have been found for obscuring the structure of a message. For instance, groups of symbols in the original message--sentences, phrases, words, syllables, or even single letters--may first be coded by replacing them with code groups of letters or figures. Either the original message, or such code groups may then be transformed, one or more letters at a time, into other groups of letters. Transformations of this type, including interchanges and substitutions for letters or groups of letters performed on unvarying units of a message together with the direct use of key constitute enciphering. Recent increases in the practicability of constructing machines which ingeniously carry out enciphering mechanically (for example, by turning wheels), or electrically (for example, by aligning contacts on wheels), or both, at a high processing rate, have resulted in a great ease in the use of encryption. Today, most [redacted]

Cryptanalysis offers some hope of success only when the ideal rules are not being observed. Fortunately, the ideal rules are not too easy to put in practice.

First, it is not quite simple to build a reliable generator for completely random key. While a number of techniques are known, our own experience with this problem shows that, unless the machine is rather sophisticated, it tends to break down quickly and produce a biassed sequence.

Second, it is difficult to prevent second use of the key. Pad systems require that as much key be distributed by courier as the total volume of traffic to be enciphered. This makes pad systems almost unusable on circuits carrying a large volume of traffic. The problem of producing and distributing pads has frequently proved insuperable and compromises have been made with the ideal rules; these compromises immediately open the system to cryptanalytic attack. During the war the Japanese frequently re-used stretches of key ten, twenty, or even one hundred times; we read a large proportion of this traffic on a current basis. For the first few years after the war, [redacted] apparently their [redacted] Key which is used exactly twice produces cryptograms which can be read only with the greatest difficulty even by very experienced analysts. Most of the intelligence gleaned from [redacted] traffic is due to this re-use of key. Unfortunately, no examples of re-use of key have been found in any [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

of finding a few more readable messages from this period and to make a definitive determination of whether or not re-use exists in the more recent traffic. If this is unsuccessful then sus-

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

tained efforts to [redacted] will be abandoned. If serious effort were then stopped, it would become important to maintain some routine check on the traffic to determine, for example, whether they switch to some other system. The Agency hopes to be able to make this watch-dog operation completely automatic within a few years.

The present outlook for [redacted] is very bleak. There can be no doubt that they are aware of the basic principles of correct pad usage and that they are now capable of producing key properly. Analysis of the key recovered [redacted] these appear to be unbiassed. There is every reason to believe that they are now operating their pad systems correctly.

At present, therefore, there is no way of [redacted] one-time communications except by gaining access to the key material and copying it without detection (detection would undoubtedly result in the key material being destroyed without use). This is one case in which technical judgment, both in the intelligence community and in this Panel, advocates [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

preferably involving code clerks who could supply not only key material but also vital information concerning its time of use.

Of course, improperly prepared key material or the reuse of key could lead to the reading of such communications. Thus, we urge continued vigilance over the whole domain of [redacted] It must be realized, however, that this involves a considerable effort.

In a one-time key system, fresh key must be supplied, usually by secure courier, at the rate of one character of key for each character of message to be transmitted. (This amount of key must be provided to both sender and recipient, and, for highest security, separate key must be provided when a sender wishes to send the same message to two or more recipients.) Formerly, encipherment was done exclusively by hand, but both hand and automatized methods are now in use. Because machine systems, where much smaller amounts of key-like material need be securely transferred from one location to another, put far less load on the secure transmission and storage of key-like material, use of one-time systems will presumably continue to be restricted to the most delicate communications. Thus, a review of the "sociology" of the use of one-time pads would be helpful. An examination of where, when, and how they are used in our, and in other, countries might give some insight into the significance of [redacted] in particular circumstances, even if the message itself cannot be read.

Recommendations

(1) Present careful scrutiny for errors in the preparation or use of one-time pad should be continued.

(2) All permissible efforts should be made to obtain one-time key material [redacted]

(3) An operational study of one-time usages aimed at deriving incidental intelligence should be considered, since no direct attack through cryptanalytic study is possible.

2. Machine Encipherment.

For many communication purposes, one-time systems are too slow and require too much key material to be useful. Thus, the bulk of enciphered material is enciphered by cipher machines. In machine encipherment the key is in principle a fairly short list of initial settings of the machine, comprising a number of characters very much smaller than the number of characters in the message to be enciphered.

A cipher machine makes use of an enciphering box which converts plain-text letters to enciphered letters. The cipher box may be operated by a typewriter keyboard and print out the cipher text, or it may be operated by a teletypewriter tape and produce electric signals which are transmitted directly. The plain text is converted to cipher text by a complicated mass of electrical circuits which are rearranged in some fairly regular manner after each text letter has been enciphered. A similar equipment deciphers by running the enciphered text through the ciphering box backwards. Cipher machines, since they operate at typewriter speeds or faster, can accommodate much larger volumes of traffic than hand systems.

Enciphering or deciphering a message requires first the cipher machine itself together with any auxiliary parts to be used with it, and second the key to be used with the individual message. This key usually consists of the selection of certain auxiliary components, the plugging of certain wires on a plugboard, the setting of certain dials, etc. In practice, certain parts of the key, usually those requiring the greatest physical effort to change, are the same for all messages on a particular day on a particular circuit, and only relatively minor changes are made in the key from message to message.

While the number of components in the key is relatively small, rarely over a dozen, the total number of different keys is found by multiplying the number of possibilities for each component and the resulting numbers may be of a size much too vast to be dismissed as merely astronomical.

Experience with Earlier Machines

The cryptanalysis of a machine system falls naturally into two stages. First, there is the recovery of the machine itself; that is, the determination of exactly how the machine works and the wiring of all circuits in the machine and any of its auxiliary components. Second, there is the determination of the individual key for each message. Because of the practice mentioned above, this usually breaks into two parts, determination of the daily key and subsequently the message keys. Understanding of the basic process is perhaps best obtained from the following sketch of the attack on the Enigma which was the principal middle-level cipher machine used by all the German military services during the recent war. Success in reading this system was almost total and may well have had a decisive influence on the war against the U-boats and the air war over Britain.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The machine itself was a modification of a commercially available machine. Through [redacted] on the part of the Poles just before the war began, the basic design of the machine and the wheel wirings were known. The key was made up of four parts: the stecker which consisted of a number of wires to be plugged, the wheel order, the ring setting, and the window setting. The stecker wires could be plugged in some 10,000,000,000,000 different ways. The wheel orders offered 336 possibilities, the ring setting, 676, and the window setting, about one-half million. The total number of possible keys is the product of all these numbers, that is about

100,000,000,000,000,000,000,000.

This number is more or less typical of the situation presented by any cipher machine. The principal thing it teaches is that large numbers, in themselves, offer no guarantee of security.

German communications procedure changed the first three parts of the key daily; only the window setting varied from message to message on the same day on the same circuit. This meant that we had to solve the really difficult problem of finding a whole key only once per day per circuit; after one message was out the rest could be read much more easily. One technique for the latter task was simply to decipher the message using every possible window setting and select the one which made sense. Since there were only about a half-million possibilities this proved to be relatively easy with high-speed electronic-mechanical equipment.

A similar try-all-the-possibilities attack on the daily key is completely impossible, since even at the highest electronic speeds we can rationally imagine it would take centuries of machine time to make the trials.

The daily break-in was accomplished by an ingenious combination of exhaustive trials and guessing. First, one had to guess the plain text underlying a short stretch of cipher. If the ring setting was favorable at this point in the cipher then it had no effect on the recovery of the other three elements, the stecker, wheel order, and window setting. An electrical circuit was devised which could test in one step all possible steckers for each combination of window setting and wheel order. The required number of these trials was then about one-half million (for the window setting) times 336 (for the wheel order) or some 170 million. A large number of special machines (called Bombes) were built which could make these trials in a few milliseconds each and an exhaustive run could then be made using about 100 hours of machine time. About fifty million dollars was expended on these machines which represented a major diversion of our electronic skills during the war.

Once the routine breaking of the traffic started a number of favorable facts were observed. The daily key lists were apparently made up in a non-random manner and this materially reduced the amount of machine time required for a break-in; diligent study of the texts of deciphered messages

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

improved our ability to make the all-important preliminary guess of the plain text underlying the cipher; certain operators were found who habitually violated the German communication rules in a way which simplified our task; etc. The over-all effect of these "dividends" was that we were able to keep current on most of the traffic from 1942 until the end of the war, in spite of the fact that the Germans introduced a number of additional complications into their usage as the war progressed.

These possibilities as discussed primarily for the German Enigma had been brilliantly made use of in other cases, as when masters of the cryptanalytic art, such as William Friedman, solved Japanese machines and early models of the

[redacted]

Unhappily, the actual readability of a message depends not only on the amount of key used, but on both the sophistication* and complexity of the enciphering machine and also upon the intelligence and care with which it is used. We may note in connection with care in use that although messages enciphered by most users of

[redacted]

this same machine. Presumably, either the messages enciphered are too brief to allow decipherment, or separate keys are used for portions of longer messages.

In fact, while a deeper understanding of cryptology and cryptanalysis tells us that machine-enciphered messages are in some sense theoretically readable, its chief practical results have been

* 'Sophistication" as used here refers to the obscurity of the

mathematical mess the machine creates in transforming plain text characters into ciphers, with economy of key. "Complexity" refers to the total expense of such a mess.

---

to provide machines which are now practically unreadable and also to show that the output of such machines cannot be deciphered by any straightforward effort of any physically possible magnitude. In particular, methods of decipherment which depend on the simple exhaustion of all possibilities can be, and have now been, made physically impossible.

Indeed, in the cases of the most complex modern machines, the only analytic source of knowledge of the construction of a machine has been enciphered when the machine was misused or maladjusted. A message enciphered improperly, or while the machine is malfunctioning, is called a bust message, and the word bust is used generally in referring to the misuse or malfunction of a cipher machine or, more generally, a system. [redacted] in the whole COMINT effort is brought out later in the report, and also in Appendix I.

Returning to the Enigma experiences, it is certainly true that the Germans could have modified their communications rules in such a way as to have ruined our exploitation techniques. The fact remains, however, that they did not. It is not easy to make a change in a major communication network even in peace time, and it is clearly much harder in war time. The changes they did make seemed to be largely directed toward the prevention of [redacted] recovery of the keys, and while they slowed us down we weren't stopped. NSA and its predecessors have [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

[redacted]

We turn now to the current, as yet [redacted] cipher machines. It is clear that it is dangerous to reason, by analogy, that because we were able to read the Enigma machine we must necessarily be able to read the undoubtedly [redacted] On the other hand, it is also clear that the resources available to the cryptanalyst are greater than may appear at first sight, and that if he once succeeds in breaking into a machine system he is very likely to be able to follow it through subsequent developments.

[redacted]

---

*Except when we told an allied government what to do.

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

The machine may or may not be in use today on the same circuits. All we know is that we have seen no evidence of the wholesale procedural confusion which usually attends the introduction of a new cipher machine.

There are at least [redacted] known under the [redacted] Of these we know the most about [redacted] and the least about [redacted] will be discussed here. [redacted] was lost. Reading this traffic may do more than restore the status quo since it may handle material which would not previously have been entructed to the airwaves.

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

are members of a family of similar devices which, in one form or another, are used by all cryptologically advanced countries, including the United States.

[redacted] came to be done with new enciphering devices which are capable of handling traffic more efficiently, and especially in larger volume, than is possible with one-time systems.

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

[redacted]

Additional features of work on [redacted] are assessed in the parts on analysis (Part IV) and development of special skills (R/D in Part VI), as well as in the following part on the [redacted]

Deciphering skills developed by struggles with [redacted] represent a resource of great value in deciphering other systems. [redacted] traffic represents a demonstrated standard of obscurity. Against this, clever attacks by applications of the deepest knowledge of language, statistics, and human cunning are being made. These have revealed approaches in decipherment which have so far marked the boundary for us and for [redacted] between the doable and the undone. Continuation and strengthening of the assault on the [redacted] traffic is vitally important to our cryptanalytic position and intelligence practices with respect to the whole world.

[redacted] its secrets. Such limited knowledge is not surprising, nor does it constitute an implied criticism of those who have worked on [redacted] It is a true measure of the difficulty of the problem.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

However, if we can

[redacted]

With the rise of cryptologic technology, the need for [redacted] information about our opponent's system is growing, not declining. [redacted] understanding both the machine and the exploitation problem its messages offer. One such [redacted] if successful, would today take us beyond where 10 years of hard work [redacted] and messages have brought us. Ten years ago, of course, such an operation would have been of equal use. As cryptographic techniques

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

and peace time cryptographic usages continue to improve, the relative value of direct [redacted] information will continue to rise. Such information need not be as definitive and complete as a [redacted] of an entire machine, or a [redacted]. A code clerk may know enough about the internal operation of the machine to be a very useful source. One [redacted] may be worth the maintenance costs of a number of intercept positions for a number of years, a substantial sum in dollars. [redacted] and valuable, but significant [redacted] which would be still more valuable, are so far non-existent.

[redacted]

a measure of either the level or competence of the effort or of its value to us, but only of the difficulty of the problem.

Both large and small powers all over the earth will soon be able to handle the bulk of their wireless telegraphy communications by enciphering machines. These will eventually provide a common high-level of communication security, even in societies where technologies remain weak. However, we may expect, provided we continue and, indeed, deepen and intensify our current work on [redacted] systems, that, during a transition period at least, many enciphered communications, and particularly the communications of the small nations which are more or less on the periphery of the [redacted] and intentions. Work on [redacted] and similar systems is justified by the important role it plays in developing and maintaining a higher and higher level of general competence, which is a necessity if these peripheral areas are to cintinue to yield valuable intelligence.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-10 USC 130
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

<u>Recommendations</u>

(1) Work on [redacted] should continue at a high pitch in order to prepare for and to facilitate the [redacted]

(2) No strategic reliance should be placed on the expectations of success with [redacted]

(3) Means which could advance the study of [redacted] traffic, noted later in this report, should be pursued vigorously.

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted] is somewhat analogous to that posed to the art of 1940 by the construction of the first electronic Bombes in England to allow the continued and adequate exploitation of Enigma traffic. While it is not clear that the large machines required for the [redacted] problem will be as valuable as were the Bombes either in terms of the amount of material read or in terms of the intelligence value of the material, the experience gained through them is bound to lead to important advances in the cryptanalytic art, and should prove especially valuable in attacking the [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted] is at hand. The most hopeful present views are

~~TOP SECRET EIDEF~~

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

5. A Revised View of Communications Intelligence Objectives.

The foregoing discussions have dealt with past experience and future prospects concerning two important [redacted] Will not an accelerated but straightforward advance in computing techniques and their application to cryptanalysis necessarily result in the solution, not only of [redacted] but of succeeding machines as well?

This problem is discussed in more detail in Appendix II, "Information Theoretic Framework for Cryptanalysis." The answer is no.

[redacted]

However, we have as yet no general method of doing this, except for the straightforward procedure of [redacted] in order. At first sight it might be thought that the advent of modern high-speed computers would make an attack based on the [redacted] a reasonable one to try. For machines of the [redacted] however, the amount of calculation required is still fantastically impossible, even with all imaginable allowance for future advances in computer technology.

Appendix II includes two computations which illustrate this situation. In one it is supposed that we know the general plan of a slightly simplified [redacted] However, it is physically impossible to carry out the computations required. Within the scope of basic physical laws there is not nearly enough energy in the universe to power the computer, itself impossible, which might do them.

[redacted] This is a more modest undertaking, and cosmic limitations of available energy no longer make it impossible. For practical purposes, however, the proposal is still fantastic. At present power rates it would still cost something like two billion trillion dollars per message merely to supply power for the hypothetical computer to do the work.

There remains the possibility that, with the use of computers, we may find some way of attacking such situations which is more expeditious than the method of enumeration of all possibilities. All hopes of routine reading [redacted] systems rest upon this possibility. Strenuous efforts in this field, however, have failed to reveal any sweeping general procedures, and there begins to be some mathematical evidence to support the idea that such general, expeditious methods may be non-existent.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

It is possible that fundamental research will lead to subtle new ways of attacking machine-encrypted material. It is clear, however, that we are squarely facing the issue as to whether communication concealed by some facility devised by the mind of man can necessarily be invaded by the mind of man. Unless startling new advances are made, the answer may well be negative. It seems that a given amount of ingenuity can be used to develop an encryption method that needs a very much larger amount of ingenuity to unravel by cryptanalysis. The offense seems to have a basic and continuing edge on defense.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

In the present, whatever outputs from the machines of current complexity are judged to be at all exploitable come from human frailities of operation which lead to one or another kind [redacted] but the more important possibility of continuing to cope successfully with the gradual advance of cryptology in other instances.

It is clear that this narrowing of the field of exploitation should not abate the energy and determination of the attack on [redacted] nor should it decrease our readiness to exploit sloppy usage which might permit reading in time of war or emergency. We must realize, however, that the slightest tightening of the [redacted] art, might deny us any immediate or perhaps eventual possibility of [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Moreover, while the situation typified by the [redacted] nations, it may be expected to apply in the future to other nations, as the sophistication of machines and practices increases. Now in the case of the [redacted] and ultimately in the case of other nations, a change in our policy position concerning communications intelligence is forced upon us.

For the foreseeable future there must be developed a philosophy of fragments, in which rare and isolated readings [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

III. COLLECTION OF INTELLIGENCE SIGNALS

1. A New Aim in Communications Intelligence.

The foregoing considerations have led the Panel to the conclusion that there must be a fundamental change in attitude and objectives in the collection and processing of communications intelligence. In the past, an overwhelming emphasis has been put on volume and completeness of interception. Today, volume of intercept is out of proportion to the value of its content.

[redacted]

and the real problem is to identify and intercept a useful sample of such traffic.

[redacted]

[redacted]

Among what traffic is available to us, it is necessary to choose wisely what should be intercepted. Some traffic, for example, that concerning [redacted] may have to be intercepted as fully and processed as speedily as possible. However, much other traffic can at best merely fill in our picture of the [redacted] and its activities in a statistical manner, and there is a limit to the volume of such material which will add materially to our intelligence picture.

Our interception should be aimed at providing the best sampling of foreign traffic, whose exploitation will yield the highest values, rather than at covering all available [redacted] signaling. What sampling is best will be discussed later in this part of this report.

2. The Cost and Efficiency of Collection and Processing.

Such considerations might have little weight if the interception of the huge bulk of [redacted] were easy or cheap. However, the present interception system is a global operation involving some [redacted] people needed to man, to service, and to

(b)(3)-P.L. 86-36
(b)(1)
(b)(3)-50 USC 403

winnow the harvest from, the presently operated [redacted] (from a total of [redacted] installed) in some [redacted] stations. The maintenance of this huge enterprise accounts for the primary expense of the communications intelligence job.

Clearly, the bulk of the material which it will be desirable or feasible to intercept and process depends on the cost and difficulty of interception and processing, and the value of any interception increases with the speed and efficiency of processing. The NSA has long pursued ways to relieve manpower, to make interception and processing more automatic in the field, and to reduce or eliminate the considerable duplication or overlapping of message catch. However, the strong emphasis on problems of [redacted] cryptanalysis together with the day-to-day struggle with an overwhelming volume of material have left too little time and effort for the vitally urgent problem of improving methods of collecting and processing intelligence.

The reorganization and mechanization of collection and processing is a complicated and, indeed, a highly technical problem. It is discussed in somewhat more detail in Appendix III. It is so vital, however, that something more should be said about it here. It involves many sorts of needs and possibilities. Among these are:

Mechanization of Morse code reception.

Investigation of whether or not an operator could use a broad-band receiver to monitor many frequencies at once.

Improvement in the quality of interception through improvement in antennas and receivers.

Provision and use of precise time-of-arrival measurements for identification of signals.

Improvements in other signal identification procedures.

Improvement in and standardization of recording means and standardization of recording in a form suitable for machine processing.

Large-scale machine processing of essentially all intercepted material.

The possibility of editing and word-recognition by machine.

One matter which deserves separate and emphatic mention is the automatic recognition of [redacted] We have seen that the only hope of exploiting the [redacted] which occur fairly frequently (about once in 350 hours of transmission). It is possible to detect most or all of these [redacted] by means of a device called a [redacted], which will soon be tried [redacted] The importance of such a device cannot be overemphasized. Its use could provide more quickly the sort of cryptanalytic material vital in the effort to exploit the [redacted] In the event that it becomes possible to read the [redacted] on the basis of [redacted], it could identify potentially readable material promptly. The development and use of [redacted] deserves great emphasis. The possibility of [redacted] detection in the overwhelmingly more difficult problem of [redacted] should be investigated.

3. Areas of Interception.

Relentless work must be continued on the interception of [redacted] links and whatever [redacted] or additional rotor machine traffic is found. In this field it appears that interception must be global, and include surveillance of all countries, regardless of present political alignments. Apparently this is an acceptable present view.

However, it appears that certain countries, such as [redacted] and others do not, for one reason or another, get real attention.

The virtual lack of interception by the United States from [redacted] is a cause for concern. A powerful receiving station in the Texas area should be valuable [redacted] Such a station could also serve as a site for field trials of antennas and other equipment.

4. <u>Importance of Consolidating Effort of</u> [redacted]

Most of the foregoing discussion has been concerned primarily with [redacted] It has been made clear, however, that most COMINT material concerning [redacted] currently comes from [redacted] interception and that we may most reasonably expect this to remain true in the future.

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

COMINT information plays an essential part in the interpretation and evaluation of such signals. Further, the equipment and personnel used for this range of intercept have so much in common that all of these intercept activities are usually carried out at the same stations as those used for COMINT signals, where the various radiations now compete for facilities and attention.

<u>The size of the job now calls for unity of effort.</u> We have seen the magnitude and cost of the [redacted] intercept problem discussed earlier. Together with this we face a tremendous volume of valuable [redacted] intercept and a great range of these other radiations. In view of the urgency of the need for information from [redacted] sources, there can be no honest and informed excuse for a duplication of collecting or processing activities, or for a scattering of talent and effort.

Technically, duplication or separate operation of intercept activities tends to put us in the dangerous position either of having every existing sort of intercept equipment assigned to each category of intercept, in order to keep current during the inevitable technical changes in frequency and modulation of [redacted] transmission, or of being left out in the cold, perhaps at a most critical time, following changes because the only appropriate equipment is used for other and perhaps less well-considered purposes.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

In support of this, we may note that Mr. Axel Jensen, of the Bell Telephone Laboratories, was told during a visit to [redacted]

Further, separation of activities into COMINT and ELINT, may lead to misinterpretation of signals even when they are intercepted. Those active in ELINT apparently define ELINT as any signal which does not <u>to their knowledge</u> carry voice or text. [redacted] signals, and particularly [redacted] might give little indication of their voice or textual character to one not vitally interested in COMINT.

The growing difficulty of intercept, as more and more traffic is carried by [redacted] and the growing variety of uses and subtlety of modulation of radiation, call for the maximum possible coordination of all interception activities in order to achieve the maximum in both penetration and utilization. [redacted] greatly strengthen COMINT activities.

Among users of foreign intelligence, single collection and processing of intercept is probably the most controversial point of the United States' intelligence practices. In this Panel, however, there is absolute accord. Based on the knowledge of 1957, and we could scarcely have reached this conclusion at an earlier date, we believe that all processing programs of COMINT, ELINT, and their relatives should be integrated under the direct control of the NSA.

(b)(3)-P.L. 86-36
(b)(1)

The natural tendency to an inadequate integration is rather unhappily illustrated by a hybrid activity at Kelly Field and at the [redacted] involving both COMINT and ELINT. Kelly Field has between [redacted] crypt-analysts and is acquiring associated machine facilities. The [redacted] professes to be interested in telemetering signals and not in digital transmission of other information, but in practice it has been unable to distinguish with certainty one sort of transmission from the other. The continued handling of ELINT material by those uninterested or not highly skilled in COMINT could leave new and perhaps crucially vital sources of information untapped.

This extra-NSA interception, handling, and analysis illustrates the close association of COMINT and ELINT in another environment. It raises a disturbing question, however--How can such activities grow up outside of the NSA when even the most the country can muster for one concerted attack is not enough?

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

There are presumably many answers to this, deeply rooted in the histories of individual military service intelligence branches and in the tensions accompanying the formation of the NSA itself. Above all, it may be in part a result of the frustration of the whole intelligence community at the inaccessibility and complexity of recent [redacted]

Among the many possible answers, however, one can be understood even if it cannot be regarded as adequate--the shrinking scale of time. As the cryptanalytic [redacted] has diminished, the natural uneasiness of the military, the feeling of a need for overnight warning of air movement has increased. As the backlog of NSA intercept presently incapable of [redacted], the internal urgency for prompt processing of intercept has inevitably diminished. By contrast, of course, the Air Force needs communications intelligence overnight. Its greatest present need is for the fastest possible processing of [redacted] in an orderly and taut traffic shop. This calls for [redacted] Indeed, Kelly Field has achieved [redacted] of much intercept once it reaches them (which may take days or weeks). The Air Force looks more and more to this source. But Kelly Field may black out [redacted] NSA must be the natural guarantor of keeping current on [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

In ways which will be examined later on, at the NSA, approval and emphasis have increasingly gone toward the tortuous and recondite work of [redacted] although traffic handing and current work have been conscientiously pursued. It is human and inevitable, however, that because of the emphasis of the difficult cryptanalytic work of PROD, a tidy daily run-down of all [redacted] traffic has not always come first.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

As an understandable but frightening consequence, the ELINT area finds about [redacted] intercept being processed in its domain. Naturally, full copies of this activity are officially available to the NSA, but the interrelation is often confined to that rarified and nominal realm of "cognizance" with too frequent loss of effectiveness.

We have seen earlier that the prospects for reading the [redacted] material are somewhat gloomy, and we have seen that we may expect that [redacted] material will be enciphered by methods increasingly difficult to read. It is tragic to contemplate the possibility that, in some time of emergency, vital enciphered material might get into the hands of cryptanalysts less able than the best at the NSA. It is even more tragic to contemplate the possibility that some misinterpretation of ELINT, or even of [redacted] COMINT, data, without the promptest and most expert evaluation in the light of all of our COMINT information, might perhaps lead to a faulty decision about national action or inaction.

The ELINT analysis functions-resolution--collation--correlation--synthesis, right up to dissemination, which is certainly the user's job, should be directly enrolled in the NSA. Indeed, the need for integration of ELINT and COMINT is well recognized and well practiced at Kelly Field. Conversely, NSA must create conditions of processing and reporting which are supersonic as well as sound. The problem is as much one of understanding and spirit as of any real deficiency, for the NSA apparently manages to keep reasonably current on the [redacted] messages a day.

5. A Collection Exercise or Catch-All Operation.

Is a worldwide collection and processing exercise an answer to the chronic issue of how a truly central agency might handle communications intelligence information promptly enough to be of tactical as well as strategic value? Throughout the military departments there is spreading, slowly but pervasively, a feeling that with the thwarting of its cryptanalytic efforts the NSA will turn more and more into a deliberative body, as far as [redacted] sources go. This impression is false, unfair, and terribly dangerous. A sense of urgency and immediacy is rampant in the NSA. Other ways to attack the question of speed of processing will appear later, but would not a realistic exercise in which most stringent military timing is imposed be valuable to see what the present NSA network could do?

Consideration of such an exercise is strongly urged. It would require, of course, a close liaison among all the services. It would be a cogent test of how the total r. lia-tion output [redacted] could be handled in an emergency. Even two years ago, at the time of the study of the Techn::cal Capabilities Panel of the ODM Science Advisory Committee (Meeting the Threat of Surprise Attack, February, 1955), our strong dependence for early warning on communications intelligence based on [redacted] The situation is certainly no

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

better now. Such a communications intelligence exercise as suggested could also incorporate practice of our decision-making ability as based on such rapid intelligence surveys.

Interesting facets of such an exercise could include [redacted] ception as well as, of course, their primary effect on our own communications. Also, [redacted] might well be inserted to test the speed and completeness with which they are handled. Such a practice operation might well show clearly that the prompt processing which the Air Force, among others, justifiably demands can already be better achieved within the NSA than at any separate activity (such as that at Kelly Field). If the exercise did not show this, the NSA would have the urgent duty to revise its operations until this was so, for the NSA has resources of technical proficiency and scope which could not be duplicated elsewhere.

In any case, the duplication of communications intelligence activity, which seems to be increasing because of accidental features of collection and the historic compromises which led to the ELINT function, should be carefully scrutinized. While [redacted] have greatly expanded the possible information content of such intercept. It is likely that voice communications [redacted] are becoming increasingly concealed. Thus, it seems that the older notions of separability of various radiation interception jobs are becoming untenable. Signal intelligence is a single field.

<u>Recommendations</u>

(1) Mechanization of intercept should be accelerated in all cases in which human judgment can be dispensed with. Available manpower should be diverted to more accurate and complete interception of new kinds of radiation and routines expected to yield the most [redacted]

(2) Sharpening and mechanization [redacted], as actively pursued at NSA, should receive additional emphasis at the expense of some of the unused volume collection now being done.

(3) All ELINT and associated operations should be fused with COMINT within the NSA.

(4) A new standard of urgency of traffic engineering, including delivery of contents to consumers, should be established in the NSA [redacted]

(5) A global exercise should be planned and carried out to demonstrate the speed and completeness of communications intelligence

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

exploitation by the NSA, particularly under simulated hostile action. This should involve demonstrations of the speed of supply to the Air Force, by a fully mobilized NSA, of detailed information on all [redacted] ingredients should be included, as well as [redacted] Fusion of these results with concurrent traffic analysis of [redacted] supplemented by whatever fragmentary cryptanalysis is possible, at the NSA to lead to the highest-level decisions would be a further valuable exercise of total COMINT capacity.

(6) From the preceding exercise, as well as from current experience, there should come an overhauling of COMINT transmission systems. Communication nets which allow proper field distribution without, logging, or being stopped by, Washington operations, should be devised.

IV. PROCESSING AND ANALYSIS OF COMMUNICATIONS INTERCEPT

1. The Need for Machine Processing.

Transferral of the intercepted signals into forms suitable for routine processing and the extraction of their intelligence content is one of the most complex issues the Panel faced. When the volume of intercept to be handled was very much less, the goal was hard copy, that is, machine-produced characters (typewriting, etc.), in contrast to handwriting. Hard copy was valued because human beings could read it rapidly and accurately. Today, because the volume of material has increased and because of advances in machine processing, the goal must be a form of record which machines canr read rapidly and accurately. Paper tape and magnetic tape on which either pulses or audio signals are recorded are possibilities. (Whenever special reading machines are economically feasible, undulator tape is also a possibility.)

The processing problem is strikingly illustrated by the case of [redacted] material, because most of chat take is currently merely fed into the super-store of backlog. Nevertheless, this type of signal requires and to a degree receives constant checking to look for evidence of machine changes, different routing practices, and so forth. We have seen that some of the required immediate identification of [redacted] should and may soon be done in the field. In the face of such extensive and difficult processing problems, there is, as yet, no plan for progressive analytical preparation of this immense supply by machine means.

Machine processing should also be used for [redacted] material. This will become possible if such material is recorded in suitable form, as discussed in Appendix III. The analysis of [redacted] which are diminishing in volume, represents an art which must be kept vigorous for the treatment of material from [redacted]

[redacted] require a still different kind of preparation for analysis which is, in this case, mostly editing, word recognition, statistical surveys, and the like. Further discussion of this is included in the next part.

2. The Place of Processing in the NSA.

Processing and analysis are primary [redacted] in NSA.

The Panel finds that research and development at the NSA has been busiest in connection with preparation of material for the cryptanalysis of [redacted] systems and in machines for carrying out some computations required by cryptanalysts. Presumably, this was considered to be the area which would benefit most from scientific and engineering studies. The research and development activities are, however, clearly identified, not as cryptanalysis, but as the provision of machines accessory to cryptanalysis, or for the preparation of material for analysis. Indeed the research and development area up to now has defined its own function as that of anticipating the needs of the PROD area for equipment, and PROD's demands have come largely in connection with [redacted] cryptanalysis.

Of course, it is not surprising that the function of processing and even analysis should manifest themselves in terms of equipment. However, we assert strongly that ideas and abstractions must be more fruitfully cultivated in some form in a research and development area. The research and development areas must develop their own view of immediate and future possibilities and needs in the whole field of data processing, and also in the field of cryptanalysis itself. In the case of cryptanalysis, a concrete suggestion will be made later.

3. The Place and Promise of Computer Development in Cryptanalysis and Processing.

Computer development is essential, but it is no longer the way out of [redacted]. We have examined the question of whether the development of analytic facilities, mostly in the form of computers optimized for the [redacted] systems, can in itself lead to a solution of these systems. We feel quite certain that it cannot.

The strategy of developing both certain special-purpose machines for comparing and counting in cryptanalysis, and the drastic speeding up of large general-purpose machines for the

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

whole complex of combinatorial problems, like cipher machine rotor simulation, nevertheless seem right in themselves. In Part II under the [redacted] techniques by computers are becoming impossible for the most hidden codes. Nevertheless, high-speed computers as early envisioned by the NSA in the [redacted] study are the essence of much hope.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Any exploitation of [redacted] will inevitably press the technological capabilities of computers to the utmost. While the nominal goal of [redacted] and while millimicrosecond pulses have been achieved using transistors, the mere speeding up of computer elements will not suffice. The Panel favors the current attitude in the NSA that more may be gained in the near future from radically different arrangements of conventional elements, perhaps combined with new devices, than from the mere such speeding up. (In the long run, both directions of advance will be combined to reach beyond the capabilities of either alone.) Certain sorts of special arrangements may come into being relatively soon, and may provide a substantial gain in analytical processing speed--a gain which has been earnestly sought for years.

However, it now appears both that the realization of the high-speed facility is far less immediate, and that the gain in total [redacted] it would provide is far

(b)(1)
(b)(3)-10 USC 130
(b)(3)-P.L. 86-36

less than had been thought earlier. Thus, while the Panel supports the planned outlay and goals for high-speed general-purpose computers, it believes that several special-purpose computers in immediate reach should not be neglected because of the promise of a 100- or 1,000-megacycle machine.

Special-purpose computers are attractive additions to the cryptanalysts' desk and mind. Keen engineering skills should be put on full use of the [redacted] editing-type machine just delivered, which was designed at NSA to read certain manual Morse codes and follow some 57 possible instructions. NSA has already conceived a modification [redacted] of this machine to record in manageable form the time intervals between reference points (axis crossings) of a signal. Since such intervals contain frequency information, further modification might yield a superbly simple and effective way of examining vast quantities of [redacted] In any case, such high-speed editing machines [redacted] has about a 20-microsecond cycle in its core memory) seem to be a principal hope of managing the flow of material that will have to be filtered if fragmentary breaks can be made into certain sorts of [redacted] traffic.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Beyond editing, however, it would seem that computer development should turn toward involvement with the senior cryptanalysts' daily work rather than toward some heroic, general-purpose, centralized machine. While the [redacted] program (with a machine perhaps 100 times the capacity of the 1103 or 704 units and an output equal to 5 or 10 of those units, as a result of improved organization, 10-megacycle logic, 2-inch wide tape with 3,000 bits per inch, and so forth) is an admirable affair deserving highest support, attention should be turned promptly toward making it available to cryptanalysts who wish to do fast but fragmentary programs. In addition, special-purpose machines, such as the [redacted] which was conceived for such time-sharing, desk-scale use, should be rapidly extended, as indeed NSA has already planned in connection with an expansion of the [redacted] type of facility.

4. The Need for Fundamental Advances in the Cryptanalytic Use of Computers.

The Panel has conveyed its specific judgments about the nature and use of machines in cryptanalysis because it believes that the central hope of eventual advance in [redacted] requires that the sophisticated cryptanalyst learn machine language and programming thoroughly enough to formulate a sophisticated machine attack on a code. This requires the solution of extremely difficult problems: the formulation in clear terms of cryptanalytic techniques, and the adaptation of these techniques to machine language or the development of an interpretive language in which they may be easily expressed--an interpretive language which machines could translate into machine language. These are problems whose solution will require much ingenuity and a great deal of time and effort. Happily, we have seen a modest beginning of this in the NSA. However, the difficulties to be overcome are far greater than the uninitiated might expect. They are not primarily problems of machine design or performance. Some at NSA have recognized this, but this recognition is yet to have its major influence on the nature and extent of what is done. A careful summary of this problem and its position at NSA appears in Appendix IV.

The Panel applauds the preperation and use of various special-purpose machines for rotor simulation, including the [redacted] and so forth. It urges that these be extended as promptly as possible to the examination of made-up problems which can furnish direct information on the cipher levels we may face as electronic rather than mechanical combinatorial devices become customary.

Recommendations

(1) Computer planning, especially in the R/D stage, should be reviewed in terms of special programming rather than of over-all (exhaustion) capacity.

(2) Closest possible connection between a cryptanalyst's formulation of solving a crypt and a general machine language to express this formulation should be attempted in new machine design.

(3) Computer facilities should be specially planned for easy use, as are some desk-access machines now available at NSA. More casual attitude toward their use than is so far thought normal should be encouraged.

(4) The planned outlay and goals for high-speed general-purpose computers should be supported [redacted], but special-purpose computers in immediate reach should not be neglected because of the promise of the former.

V. FOREIGN INTELLIGENCE SOURCES SUPPLEMENTARY TO [redacted] [redacted]

1. The [redacted] Sources.

Presumably the information contents of many secret messages are actually reflected in masses of accessible communications. Despite the nearly perfect concealment of [redacted] communications for the past several years, the intelligence community has nevertheless been getting important indications of [redacted] Since the Panel has emphasized fragmentary reading as the most we should expect from [redacted] ciphers in the foreseeable future, it may be important to look into the technology of the thriftiest coupling of whatever [redacted] information there is with the great mass of [redacted]

Indeed, comparatively little is known about the realities of such coupling in an autocracy like [redacted] It may be that a useful political science-economics study could be made of the way [redacted] decisions and actions are anticipated or reflected

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

by a mass of disseminated [redacted] instructions and exhortations. While such a study has of course been imagined by people at the various assessment agencies of the security group, there has not been a careful reconstruction of a series of periods such as in [redacted] connected with [redacted] Any principles derived from such a comparison would be of vital and immediate usefulness now and in the future.

Beyond this sort of qualitative consideration lies the problem of actually sorting through [redacted]

We should also keep in mind that [redacted] and many routine [redacted] activities are regularly deciphered from [redacted] systems. Presumably similar codes are concerned in the U. S. [redacted] and in certain of their internal communications in [redacted]

<u>Thorough abstracting of</u> [redacted] <u>may reveal intelligence traditionally sought only in</u> [redacted] In all handling of these auxiliary sources of intelligence there is supposed to be rigid adherence to the Users COMINT Objectives List of some 12 items. A disturbing unreality persists in such a single list of objectives, which tends to concentrate attention

on certain pre-eminently important things which would be directly obtainable only from some [redacted] Today, approximations to some of the information sought are derived in a left-handed way from a bulk of only partly assimilated material. Supplementary, adjustable priority decisions probably do, and surely should, take account of real rather than ideal exploitation. The Panel believes in the immediate importance of an operations analysis type of study aimed at bringing the mass production application of the Objectives List into line with the best content of the [redacted] content of several hundred thousand [redacted] messages per month.

As Appendix IV on programming brings out, there is important progress in the NSA toward machines which can rapidly exploit [redacted] It should be possible to convert such messages to [redacted] text by machine and to employ speedy methods for scanning the large body of such copy in conjunction with the scanning of [redacted] interception. The [redacted] scanners now looking for special words in [redacted] ought as soon as possible to be supplemented by word-recognition machines. A possible design for such devices is discussed in Technical Adjunct II.

Evidently, the filing and cross referencing of information after it is completely read is alone a formidable operation. It too must have improved machine treatment such as can neither

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

be obtained nor afforded by separate activities in a Kelly Field or other military headquarters remote operationally (for geography is of much less significance) from the NSA resources and skills. Nevertheless, here, too, Kelly Field does a prompt, well-managed job of reference assembly which is a stimulating, if limited, example.

An expanded body of strictly current operations from the [redacted] will be good for COMINT vigor. Such an objective will also clearly favor the rapid processing and analysis essential for proper use of the ELINT intercept.

2. Urgent Current Values of [redacted]

Proposed [redacted] and commercial operations into 90 principal districts may temporarily enrich the content of [redacted] cipher systems. It is understood that, while raw materials, manufacturing, and merchandizing or distribution activities will be controlled locally, the research and development functions for industries will be approved from [redacted] headquarters. Apparently, traffic concerning development activity has often yielded the most accessible and interesting communications such as that concerning the early [redacted] and so forth. Conceivably, an important period accompanying the [redacted] could now be starting. Doubtless, much of the communications concerning this will be sent via [redacted] and particularly via the rapidly strengthening [redacted] noted earlier, but for the next few years there may be exceptional values in more massive and detailed attention to the bulk of material that has previously necessarily been somewhat spottily treated.

Filtering of all grades of ciphers for information values seems important in [redacted] other changes. Similarly, the expanding communications in [redacted] while subject to large fluctuations in both accessibility and interest, should be handled by such semi-routine mechanized surveillance methods. The attitude in this whole area is dominated by the consumer demand for occult and (perhaps uncommunicated?) military information. The conscientious staff thus becomes obsessed with ciphers--the more difficult the better. A group intellectually suited for crytpanalysis must be strengthened for that task, but hundreds or even thousands of others in COMINT should feel equal emphasis on assimilation of existing, accessible information.

It would be interesting to know what tactics the [redacted] find most efficient in using the great bulk of military and commercial intelligence that the free world openly communicates and often publishes in papers and journals. What filtering system is applied, say, to the *New York Times*, or *Aviation Week*?

3. Auxiliary Sources of Intermediate and Minor-Grade Codes in Coded Communications Intelligence.

Relations of the NSA and other parts of the intelligence community with allied nations seems already of great technical value and should be discreetly expanded.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

We have long linked [redacted] integrally with much of our activity. As was convincingly implied in the report of [redacted] to Director of NSA, [redacted]-US cooperation is a tremendous adjunct to our own highest skills.

Our contacts with communications intelligence practices and techniques in other [redacted] countries like the [redacted] are rewarding, especially in connection with [redacted] systems, and should be cultivated.

VI. NSA--THE NATIONAL RESOURCE FOR COMMUNICATIONS INTELLIGENCE

1. The Need of a New Pattern for the NSA.

The Panel finds that the National Security Agency has one of the highest levels of technical efficiency of any Government office and deserves the unqualified support of the military and civilian complex concerned with our political and strategic policy. This judgment is based partly on a clear and forceful impression of the competence, intellectual stature, and devotion and effectiveness of the staff, but it also rests on firm scientific bases, including evidence that information on weapons and logistic capacity comes more definitely from communications intelligence and properly related ELINT effects than from any other source.

As noted in the Preface, the Panel's recommendations about the NSA involve shifts of emphasis and organization which are related to a view of its activities appropriate to the situation which it faces today and must face tomorrow. It is not within NSA's province to make these shifts either on its own initiative, or on the recommendation of any advisory group. Only clear leadership and guidance from the sources of its most basic policies can create a situation where these shifts will not only be possible, but administratively obvious.

Given such "guidance from on high," a most fundamental change in outlook can, and should, be accomplished. Central to the NSA as a researching, developing, producing, continuing organization is the ideal image of what the NSA should be, not only in the eyes of its administrators, but as seen by all of its informed personnel, especially the many thousands of informed members of its Washington staff. Such an image can draw NSA ahead, hold it back, or even destroy it.

Thousands of NSA employees are most devoted and intelligent public servants, skilled in technology or administration. They are largely denied the satisfaction of public recognition of

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

evident accomplishments. Indeed, they are generally denied even the satisfaction of being known to be working on an important problem for the public good, as would be the case if they worked at Los Alamos or Ramo-Wooldridge. Naturally, they have sought, and continue to seek, the best available substitute. Through this search for recognition and approval, they have tended strongly to identify the achievements of the Agency with the astounding war time accomplishments of a tiny group of inspired and eminent cryptanalysts. The supply to our military and diplomatic heads of the inner secrets of other powers was a war time service which cannot be overestimated, one that cannot, and should not, ever be forgotten.

However, over the past decade, notwithstanding the constantly increasing skills of our cryptanalysts, our access to the [redacted]

Naturally, the ambition to regain this access and the search for way to do so, in order to continue to deserve the confidence which they have won, still constitutes a driving force for the NSA, which accounts for many curious features of its organization and operation.

Today, the larger part of the prime intellect and leadership of NSA is concentrated in the ADVA section of PROD. (This, of course, is the part of PROD which is least concerned with "production.") Yet the enterprise and courage so strongly displayed here are desperately needed in other parts of the Agency's operation.

It seems almost as if memories of successes in earlier, simpler times have created a Frankenstein-like monster which amasses constantly greater heaps of material which a dozen or 20 cryptanalysts, experienced and capable of attacking such material, cannot even lift, let alone survey.

Conversely, the most pressing problem of the Agency, the great organizational and engineering challenge of exploiting quickly, wisely, efficiently, and as fully as possible, all of [redacted] which are currently actually or potentially useful, has come as a necessary but not welcomed diversion to the most skillful and original intellectual leaders in the Agency. NSA has most characteristically, under both its military and civilian leadership, worked manfully despite this condition of split personality, but its full potentialities in contributing to the national security cannot be realized without a reorientation in the thinking and attitudes of its leading spirits, a reorientation on which corresponding reorganizations of structure and function could be profitably based.

<u>2. Broad Problems of NSA's Research and Development Activity.</u>

The research and development organization has, wisely, been encouraged to take a leading part, in cooperation with the other parts of NSA, in planning and supporting NSA progress. Top administrators in the Department of Defense and the NSA have given most thoughtful and devoted attention to the support and growth of the R/D organization. The evidence and the record make it clear how thoroughly Lieutenant General Ralph J. Canine saw and understood the deep need, in a central communications intelligence organization, for a vigorous research and development organization. Great strides were taken during his term as Director, but, as General Canine pointed out in his testimony before this Panel, the job is far from complete.

The need for adequate contacts with extremely competent outside scientists and engineers was clearly recognized at an early date, and the official position of such consultants was strengthened by the setting up, in 1953, of a Scientific Advisory Board composed of eminent academic, government and industrial scientists, and assisted by panels of consultants in mathematics, electronics, and telecommunications. By and large, however, the members of this Board continued to operate as individual consultants. Besides the Robertson Report of 1953 on COMINT as a source of early warning, the only example of a collective study of a broad area of NSA activity would appear to be the 31 May 1957 report of the Scientific Advisory Board's Mathematics Panel on the use of mathematics and mathematicians throughout the Agency. We hope that the clarification and readjustment of NSA goals, recommended in our report, will be accompanied by a strengthening of the Scientific Advisory Board as a source of working groups concerned with the technical aspects of many more broad problems within the Agency.

While the top administrators and the Scientific Advisory Board continued to emphasize the central role of research and development in NSA affairs, the necessary persons, experience, ideas, and insight could not be created overnight. In partially adapting itself to new times and new problems, the NSA faced obvious problems of development. It was natural, and we believe wise, to press first and hardest on development. However, General Canine, himself, has expressed to us his belief that research has lagged, and that this should be corrected.

In part because of a sequence of fateful events, partly triggered by the emergency conditions of the [redacted] aggravated by many changes in top personnel, the intention that the research and development organization should play a central role is still far from realization. While there is continuing and, in many respects, effective build-up of the R/D program, the R/D organization seems never to have assumed the necessary leadership in forming a pattern for the steady renewal of NSA.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

We should emphasize that this has not been because of lack of over-all support in either funds or people. While further expansion is currently sought, the continuing growth of the R/D operating budget [redacted] in 1957), together with the present size of the organization [redacted] shows that administrative support of the R/D complex has not been absent.

What has been absent has been a recognition of NSA's role in a new era and, specifically, a recognition that research as contrasted with both production and development, is an essential, central function of NSA; a function which must be carried out well if NSA is to do its best against the mounting challenges it faces. In less vivid terms, the difficulty has centered in the internal aims and emphasis of the R/D organization. There have been pressing diversions from the path of forward-looking leadership. In particular, as explained above, it has been quite natural for the mathematical research group to turn toward PROD problems, instead of systematically attacking certain basic problems of cryptanalysis,* and for other research and development groups to turn toward the recent exaggerated emphasis on machine design. Accordingly, there has been little chance for any substantial part of the whole R/D organization to think and act together toward integrated progress of the NSA.

Because of this situation, the Panel recommends rather drastic proposals for strengthening this part of the COMINT effort. These are drastic in that they call for unusual organizational action, but they continue the orderly growth of the past insofar as aims and techniques are concerned. They are in line with the

* These are reviewed in Technical Adjunct III, Estimate of Technical Situation in Cryptanalysis.

need for strengthening research which has been clear to key administrators in NSA, as evidenced by such far more drastic proposals as PARALLEL.

3. Brief Discussion of Certain Aspects of Current R/D.

As a background for the proposed changes, we need to discuss further examples of present R/D work. Part IV has already treated activity in machine design and performance, as it arose in connection with processing and analysis, although attention was not there drawn to the unfortunate division of machine development activities between MPRO (in PROD) and such R/D constituents as AHEQ, MODL, and ENGR.

The basic science groups in R/D deal principally with physics and mathematics. Physics is supporting, with justifiable pride, a number of important academic researches. Those devoted to the upper atmosphere, with their implications for propagation of signals, antenna performance, and related basic factors in interception, seem appropriate. Such suitability is also apparent in certain programs on theoretical physics, such as the N.Y.U. work on Maxwell's equations, although the quality and orientation of such studies might be improved. The work in the field of solid-state physics is discussed briefly in Technical Adjunct IV.

Engineering research activity in R/D illustrated how alert observation of what can be learned from external sources can be of the greatest value. The preoccupation of one group with certain components for high-speed machines, especially with

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

those usable in electronic rotor simulation, is of top value for the NSA. This is exactly the sort of junction with outside unclassified activities that should be firmly and steadily supported. For instance, electronic rotor simulation involving millimicrosecond pulse rates and megacycle stepping rates can and should interact strongly with modern communications developments for pulse generation and handling. Further, such techniques could inspire systems for COMSEC which would protect our position for years to come and at the same time give us possible insight into the most threatening machine advances by foreign powers.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The [redacted] computer program affords an important illustration of how the program of this part of R/D should be revised, once the revised objectives for the NSA are put in force. The goal of the 1,000-megacycle repetition rate can no longer be regarded as a near magic solution to the problem of breaking [redacted] ciphers. Thus, a back-breaking effort to achieve a computer of this capacity is unwarranted. On the other hand, a shrewd, well-engineered advance toward this goal should be of tremendous over-all importance to COMINT's general capability in the years to come. From this broad view, however, the effort should be to establish a new level of computer design, such as recent conceptions of microwave logic appear to offer, rather than to rush a computer to completion by an extravagant expenditure of both money and of our technical resources.

In contrast to some of the research discussed above, some of the mathematical work (and some closely related work) in R/D is

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

clearly pointed toward the best interests of NSA. The Panel's interpretation of the interests and activities of this group indicates good insight into the basic needs of [redacted].* This sounds less than startling, but it is significant as pioneering a new emphasis at NSA. In their four divisions, of cryptographic, cryptanalytic, statistics, and methods research, NSA's mathematicians have begun a systematic formulation of cryptanalysis that encompasses many of the improvements advocated in our discussion of processing and analysis in Part IV.

The statistical division's achievement of a program for [redacted] is a beautiful single example of what must be repeated many times in the future. This was the sort of capitalization of learning about the fundamentals of sophisticated machines referred to in earlier parts. Further, [redacted] by means of this program actually has found intense application during the [redacted] in reading messages which were inaccessible to earlier techniques. Further significant progress has been made in another connection with the [redacted] in which programming techniques exhibiting some of the human judgments of the crafty analyst are attained. This work seems to have, in NSA opinion, something of the position of harmless but not

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

*The Panel agrees generally with the recent report of the Mathematics Panel of the NSA Scientific Advisory Board (31 May 1957) on the need for and progress toward "a unified science of mathematical cryptology."

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

first-order activity, but, to this Panel, it appears to be closer than anything else to the sort of basic work which the Panel believes to hold the best hope for progress in communications intelligence.

4. Needed Changes in the Basic Segmentation of the NSA

The next logical development, once the central role of research for NSA is recognized, is to accentuate and strengthen research. That this will require the bringing together of the best research abilities of the NSA is obvious. That this will require a separation of research from development is not quite as obvious, but the Panel's studies have indicated this to be equally necessary; in fact, the Panel has become thoroughly convinced that this separation will have to be organizationally deeper than the Panel believes likely to be possible without special action. The basic subdivision of communications (and, as elsewhere recommended, elctronics) intelligence activities should thus be into production, development, and research. All three of these fields of activity should be recognized as of crucial importance to NSA's continuing functions of supplying critical intelligence.

The Institute for Communications Intelligence Research. The central proposal directed toward sharpening and accelerating the NSA assault on [redacted] is the establishment of an external-internal organization for research (a cover name should perhaps be used). This organization, like the AEC's Los Alamos Laboratory, or the DOD's Weapons System Evaluation Group, would be operated under external contract in close association with all the rest of the NSA.

Such an organization would differ from that proposed in PARALLEL, in that, like Los Alamos and WSEG, its personnel would deal with the substance as well as the abstractions of NSA. This substance would mainly consist in dealing with the most difficult ciphers, though but not beyond the point that they were broken or reasonably penetrated. The branch would be composed primarily of the mathematical and basic research parts of R/D and the bulk of ADVA from PROD. Its leadership and staff would have professional and economic levels fully comparable to the best scientific activities anywhere in the nation. This has indeed quite generally been maintained at Los Alamos, despite the high secrecy necessary there. It is believed that the growing activity in the country in the communications field generally, and in computers and data handling, in particular, will provide an increasingly satisfactory interaction for the professional expression of many members of such an NSA branch, even though most of its work is highly classified. That is, there will still be a chance for scientific exchange with, and invigoration from, rapidly growing collateral activities. This could, and should go considerably beyond even the praiseworthy but relatively constrained SCAMP effort.

This proposal would overcome the somewhat confused objectives which now exist in the NSA structure as a result of the sincere and diligent efforts of its leaders to adapt it to the bewildering rapidity of change in demands and pressures which it has felt almost weekly in the tense and speedy atmosphere of foreign affairs since Korea.

By this proposal, the whole remaining structure of NSA would be readied for a unified and precise adjustment to the needs and opportunities of the day-to-day communications intelligence struggle. Further adjustments may be considered in order of their separation from the Institute for Communications Intelligence Research proposed above.

Development of COMINT Apparatus and Systems. The offices of the R/D organization not included in the new Institute, and certain sections of the four PROD support offices involving development programs, especially a considerable part of the existing activities of MPRO, should form the development organization of NSA. This organization would have the highest calling to transform knowledge and apparatus designs into practical and usable form. Presumably, this organization would serve both COMINT and COMSEC. It would provide the best facilities for encryption, decryption, processing, and interception that can be attained. Above all, this organization would have a chance to evaluate and to select objectively from the very best from the vast complex of mathematics, physical science, electrical and mechanical engineering, and systems research that is daily accumulating in communications and data-handling fields. This selection and exploitation cannot be done while the development effort is dispersed and precommitted, partly by fusion with the basic research program and, even worse, by fusion with operating divisions, such as PROD and the COMSEC production area.

(b)(3)-P.L. 86-36
(b)(1)

Activities of the COMINT Production Organization. The functions of the seven PROD offices besides ADVA, as defined in the COMINT Production Organization Manual and exhibited in various conferences with the Panel, appear to cover the technology of the appropriate areas which can give the best intelligence yield. Critical in this, the major, part of PROD is mostly the need to apply the highest efficiency of modern systems engineering. This does not imply deficiencies in the current administration, but rather a basic reorientation of the motives for PROD, taking into account the patterns discussed in the beginning of this part and elsewhere in the report. Throughout the personnel of some [redacted] members, including both civilians and military, spanning the widest imaginable range of training and instincts, there must be implanted a uniform conviction of urgency and currency--a certainty that they are dealing with the possible and the immediate. This sounds naive when we know that under any conceivable circumstances a large part of the actual work of PROD offices, such as COLL, [redacted] and perhaps ALLO, are inevitably to build up backlogs. Nevertheless, the attitude can be that even a backlog should be built quickly and, as far as handling of raw intercept goes, the more backlog the more merit! This, of course, would be backwards from the present system, in which the final reading of the hardest, and hence most belated, code is the essential gauge of merit in PROD.

PROD is, after all, the shadow of the military intelligence groups collected together for the NSA. System rather than content

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

is naturally the criterion for building up the confidence of the diverse military consumers. Their traditions are such that without an explicit, rapid, current, defined system of communications intelligence production they will be unlikely to rest content with any amount of technical excellence in [redacted]

5. Relation of NSA to Programs of Other Agencies

Stern emphasis has been put on the finding that we can really support, at least in brainpower, only one NSA. However, the conscientious centralization of communications intelligence really also means, and demands, refined coordination with other intelligence agencies, particularly CIA and FBI. Earlier discussions accented the remarkable values that [redacted] activities related to COMINT now assume, with single machine patterns aiding access to hundreds of thousands of messages.

The Panel believes that technical advances should attract more and more collaboration between NSA and CIA. Detailed planning of agent operations is, of course, not an area for NSA participation or cognizance. But the technical techniques of [redacted] interception, such as [redacted] can be improved through close technical collaboration between representatives of COMINT, COMSEC, and various branches of the CIA.

[redacted]

[redacted]

Judgments of the Panel concerning scientific aids for [redacted] activity are available separately from this report. However, in specific applications to communications intelligence, such as observations of code books through safe unlocking, we believe the FBI capabilities are excellent. Full support of them, with better extension of the FBI scientific work to other parts of the intelligence community than now exists, is imperative.

Nowhere in the U. S. intelligence community is there even a small group concerned with a continuing intelligence study of foreign cryptology and communications security procedures. In such a field as biological warfare, for example, groups actively study current developments and endeavor to predict future weapons and dangers. But in cryptology and communications security, a field whose greater importance is budgetarily clear, we do nothing explicit to obtain a basis for preparing for the future. This gap in U. S. [redacted] intelligence activities may well have occurred because the boundary between NSA and CIA was hazy in this area. The Panel has no recommendation as to <u>where</u> this work should be carried out, so long as liaison with both organizations is intimate. The Panel does feel strongly that this sort of work should be undertaken somewhere.

<u>6. Brainpower at NSA</u>

Over and over, the Panel has asserted that whatever strengthening the nation can hope to gain from [redacted]

(b)(3)-P.L. 86-36
(b)(1)

exploitation depends on a handful of dedicated experts. Although we advocate a new institute led intellectually by these experts, others long before us saw that the species must be propagated as well as appreciated! Thus, NSA, and particularly General Canine, in the past six years or so, have mounted one of the most noted recruiting ventures in the Government. While the number of "good professionals" is said to have been tripled already (to a total of about [redacted] expected to become top-level cryptanalysts, of ADVA stature), there are still only [redacted] experienced enough to effectively advance the [redacted] work.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

For reasons related to the Panel's profound conviction that unabated assault on [redacted] material is requisite for our national position in cryptanalysis, reenforcement of this select group is urgent. Of course, that is the intention of the continuing recruiting program but the timing is such that we hope there is currently a positive test of whether new generations of cryptanalysts will be evolved comparable to the present remarkable dozen.

All the techniques used in academic and industrial research to develop youngsters into outstanding research men, including a proper use of the apprenticeship relation, should be applied by NSA in the cryptanalytic field, as well as in other research areas.

Studies at the NSA about the "psychology of cryptanalysts" may ultimately help to identify them among the population at large. But we look for immediate assurance that through calamities of illness, etc., the tiny, critical core of existing skills does not vanish. Even the communications intelligence capacities we think we have could then vanish too. (Some of us have talked to Panov, head of the "Information Institute" in Moscow; his enrollment seems to be rising fast.)

<u>Recommendations</u>

(1) Research should be recognized, alongside development and production, as a prime activity of NSA. This recognition should be implemented by an organizational separation between research and development.

(2) The research organization should unite the basic research now in R/D and the most subtle cryptanalytic work, now in the ADVA office of PROD.

(3) The mathematical part of the research organization should seek promptly to develop a basic mathematical foundation of cryptology. Many valuable steps toward such an achievement have been pointed out in the 31 May 1957 Report of the Mathematics Panel of the NSASAB.

(4) The research organization should be set up as a contract-managed research agency on the general pattern of Los Alamos or the Weapons Systems Evaluation Group. Like these institutions, the research organization should not confine itself to abstractions, but should be closely related to NSA's basic problems, differing in this from such

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

conceptions as PARALLEL, but resembling them in that it should carry out the attack on the [redacted] problems.

(5) The leadership and staff of this research organization should, moreover, be on an economic and operational basis equivalent to the best industrial and academic institutions.

(6) The development responsibilities of the NSA should also be consolidated. In particular, these will involve the development of both analytic and processing machines, new cryptographic systems, and new systems of data handling. Components from R/D, from COMSEC, and from certain sections of PROD, such as MPRO, will certainly be involved.

(7) The revised Production organization should establish expedited systems of intercept processing and analysis so that its gauge of performance is currency of reporting rather than a mixture of this with depth of reading, as is the present practice.

(8) By systems engineering techniques, PROD should create procedures whereby intercept analysis is continuously provided for military surveillance, even if the information provided is limited to traffic counts or even to statements of the existence of foreign links. This means that rapid systematic criteria for assigning intercept to

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

differentiated backlogs and quickly applying the most probable time-for-reading label for various classes of intercept are essential.

(9) Technical cooperation between NSA and CIA should be greatly improved, because cryptanalytic values of [redacted] are so great.

(10) A small group concerned solely with intelligence about cryptology and communications security practices should be established within the U. S. intelligence community.

(11) Especial attention must be continually given to the recruitment of potential top cryptanalysts, and to their development after entry into NSA, as by apprenticeship techniques.

APPENDIX I

THE VALUES OF [redacted]

A [redacted] that is working imperfectly, either because of mechanical failure or from operator error. Sometimes, for example, identical copy is [redacted] in the copy or in the circumstances of its transmission. Great effort is being made to [redacted] would be most valuable.

At present, estimates of [redacted] traffic sent in some [redacted] range as high as 20 per cent, but a more reasonable figure would be about 3 per cent. That is, if we did find a solution to the use of [redacted] we should have access to at most 3 per cent of the traffic, and we should have no choice as to which 3 per cent this would be. It would be, however, clearly a fabulous step forward.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

It is sad but true that, thoug[redacted] to date have given us a fair amount of knowledge about the [redacted] machines, they have [redacted] Indeed, there is absolutely no promise that they ever will. Time is against us in the following ways:

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(1) The [redacted] cryptographic systems are more and more likely to undergo small but crippling changes (such as new sets of wired wheels), thereby rendering [redacted] more difficult to utilize.

(2) The useful data that can be gleaned from our present store of copy becomes increasingly outdated, and presumably the [redacted] operators will make fewer mistakes and hence the frequency of [redacted]

On the other side:

(1) The size and capacity of our computers is increasing enormously, and with them our ability to handle such problems.

(2) Our store of copy is also steadily increasing.

(3) In the few historically comparable cases the [redacted]

The intense study at the NSA and by outside study groups (SCAMP) has not only shown no sign of any easy or accessible vulnerability in cryptographic systems as well designed and used as the [redacted] ones, but it also suggests that such a vulnerability might in fact not exist. We should note that to a large extent our own secrecy systems are very similar to theirs. One is led to consider exhaustion techniques, which are exhausting not only to the system being solved but also to the analysts. This matter is discussed in detail in Appendix II, "Information Theoretic Framework of Cryptanalysis." Although in [redacted] the number of alternatives may be cut down very substantially, nevertheless it is not clear that exhaustion solutions of [redacted] are within the bounds of feasibility, even with the faster computers to be available within the next five years. Short cuts to the reading of [redacted] which will by-pass the deadly path of exhaustion must come, if they can come at all, by fundamental research in cryptography and in machine cryptanalysis, or from [redacted] information about cipher machines.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

A decrease in the [redacted] is not an idle prognosis; it is an established fact. The frequency of recognizable [redacted] is slowly decreasing. We may hope that automatic techniques will lead to automatic recognition of many [redacted] that otherwise escape detection and so increase the [redacted] available to us, but there seems to be little reason to suppose that this will in the long run increase the total rate at which [redacted] become available.

It should naturally be emphasized that any sudden change in [redacted] activities (e.g., the [redacted] usually produces a [redacted] of all kinds, including outright transmission of

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

clear text. Association of [redacted] situations heightens the importance of [redacted] identification and analysis.

The sensible course of action seems to be to maintain a state of reasonable alertness for [redacted] in the field, and meanwhile to work toward a mechanization of that alertness. It is probable that any solutions will come, not from a breakthrough following a flash of genius, but from diligence and care with modern computers.

It should be kept in mind that, even if solutions do ever come from [redacted] situations, this would not result in a prompt flood of clear text. Each solution would probably take a considerable time, and, in any case, the frequency of solutions that can be expected is likely to be small.

The main value of [redacted] yesterday and today is likely to be their main value tomorrow. They have served, and we may expect them to continue to serve, as the main source of information about the structure and peculiarities of otherwise unknown cryptographic systems. The information they have produced has not been duplicated, either as a whole, or in substantial part, by any other source. They are the main food of cryptanalysis. Great efforts to recognize [redacted] especially during the early usage of a new system, are extremely valuable.

In summary, there is justifiable but faint hope, and only small expectation, that [redacted] as presently recognized and handled, will produce readable text from [redacted] copy. The present frequency of [redacted] may well fall, and it cannot be expected to rise, except during crises or in time of war. The hope we have of more effectively exploiting [redacted] lies mostly in increased and cleverer use of machines (computers) for their recognition and analysis. [redacted] are by far the most valuable source of cryptanalytic information we have, and their early identification and broad coverage is, and will remain, very important.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

APPENDIX II

INFORMATION THEORETIC FRAMEWORK FOR CRYPTANALYSIS

Recent years have seen considerable progress, particularly on the mathematical side, in our basic understanding of cryptanalysis. This understanding can conveniently be summarized in terms of the concepts of modern information theory, though most of the advances actually took place well before the formulation of the theory.[1] The problem of cryptanalysis may be formulated in information theoretic terms by the simple observation that to decipher a message we need information on the type of enciphering system and the particular key used. Such information must, in most practical cases, be recovered from the intercepted message itself.

In terms of information theory, however, the quantity of information in a message is related to the *a priori* statistical structure of the ensemble of messages of which this message is but one representative. It is only by the relation of the message to some conceivable ensemble that we can learn about the system from an encrypted message. At one extreme of such structure we have purely random sequences of characters akin to random noise in electrical communication. Any message encoded by means of completely-randomly-produced one-time key has such a completely random structure. At the other extreme we have, in messages produced by certain simple schemes of enciphering, statistical departures from randomness in

---

1 C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, Vol 28, pp 656-715, October 1949

such simple characteristics as frequencies of certain individual characters or of certain pairs or triples of consecutive characters. Any statistical structure of the enciphered text, such as a predominance of one letter, of certain pairs or triples of consecutive characters, too frequent repeats of the same character at certain critical distances, etc., represents a reduction of actual information content from the limit of a random sequence.

If a language had no statistical structure, zero redundancy as the information theorists would put it, there would be no possibility of decrypting an encoded message. In other words, the information content of the intercepted signal would be all used up by lack of knowledge about the message itself. There would be nothing left over to help the cryptanalyst to determine the key. Any possible key he chose would lead to a plausible message, and there would be no way of distinguishing one such from another.

Formal information theory does not usually concern itself with the actual meaning of the message. Thus "roses are red" and "please send reinforcements," which are both good English, would be equally admissible for many purposes. In principle, however, the a priori statistics of the actual messages are also important, and the fact that a message sent over a military communication link normally has to do with a military situation cannot be ignored. The power of cribbing in cryptanalysis depends on this. It represents the introduction of message statistics in a particularly strategic way.

Information rate, redundancy, and their sum, information capacity are usually described as so many bits per character (per second, etc.). One bit represents a single binary (yes-or-no, zero-or-one) choice. Ten bits represent ten such binary choice, or the equivalent choice of one out of a thousand alternatives (precisely 1 in 1024).

The redundancy of English has been calculated in various ways by Claude Shannon. The limiting information content of messages in written English text is about 5 bits per character (since the number of possible characters is about equal to 2^5). If we consider only elementary statistics, such as individual letter frequencies, the redundancy is small, of the order perhaps of a bit per character, but it grows steadily as the complexity of the logical structure considered increases. Shannon has found,[2] by indirect means involving the use of human subjects to guess the continuation of a message, that in long English messages the redundancy reaches an asymptotic value of at least 3 or 4 bits per character, so that the actual content of new information appears to be around 1 bit per character. This shows that there is a great deal of statistical structure in English text (and similarly in other text). However, this structure is not easily described, particularly since we don't know just how a human subject is able to use the totality of his past experience in extrapolating such messages.

---

[2] C. E. Shannon, "Prediction and Entropy of Printed English," Bell System Technical Journal 30, 50-64 (1951)

In any cryptological system use is made of a certain amount of key in enciphering a message. In one-time encipherment a character of randomly produced key is used in enciphering each character of the message to be transmitted. One-time key systems are theoretically and practically unbreakable if proper key is used (and if the key is used for one message only).

In passing, it should be noted that the practical utility of [redacted] minimum length of message which cannot be in practice deciphered. This fixes the frequency with which the key must be changed, and, since the transmission of new key is equivalent to the transmission of one-time key material, measures the relative practical advantage of a cipher machine over the theoretically perfect one-time system. For example, if the message redundancy were 50 per cent, and if we assumed that a message could be deciphered at the minimum theoretical length, we would find that the length of message which could be transmitted before the key had to be changed would convey only twice the information content of the key itself. The practical advantage of a theoretically unbreakable cipher machine over one-time key would be minor if this were the case.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

In all systems which are practical for volume traffic, such as [redacted] a comparatively small amount of key is used in enciphering very long messages.

According to Shannon's theory, a coded message becomes decipherable, roughly speaking, when the message is long enough so that its nominal information content (without redundancy) is equal to the actual information content of the clear text (including redundancy) plus the information required to fix the key. Thus, because of the redundancy in the clear text we accumulate a certain amount of information, character by character, until we have just enough to solve the problem. Messages shorter than this are undecipherable, because many keys will lead to valid plain text, and we have no way to choose among them. Messages longer than the critical length contain a surplus of information and should therefore be somewhat easier to decrypt.

At the critical length, where we are essentially using all our knowledge of the language to solve the problem, the procedure of decrypting is essentially one of simple enumeration of all possibilities, to represent the single one which statistically speaking, is valid plain text.

Here we have assumed that we are using all our knowledge of the statistical structure of the clear message. However, the same approach should work if we deliberately make use of only a portion of the actual statistical redundancy in the original message. [illegible] example, while English text appears to have a redundancy of 3 or 4 bits per character, we might make use only of simple character frequencies, equivalent to a redundancy of 1 bit per character, and still hope to read the text by going to messages 3 or 4 times the length of the necessary minimum. To carry this sort of reasoning to the ultimate, for example, we might conceive of decrypting extremely long messages enciphered character by character from English plain text merely from the fact that, in the English language, u follows q almost without exception.

In cryptanalytic practice we see the same situation as in Shannon's work. Single character and character-pair frequencies are used explicitly and in understandable ways. Cribs (likely words or phrases) are chosen by the aid of unformulated, and so far unformalizable, rapport with the sender's likely messages. Other delicacies in the statistical structure of language are used subtly and with much human cunning. No one has yet identified the subtler structures of language effectively; such techniques are still far from the possibility of machine use.

In dealing with specific problems of cryptanalysis we can draw certain valid conclusions from the concepts of information theory if we properly identify the meaning of key. In essence, the length of the key might be defined as the number of characters needed to give a non-redundant description of what we do not know about the machine used to encipher the message. Such a description would be shorter, for instance, if we knew that the rotors of the machine were chosen from a limited set of wirings than if we allowed any possible wirings. If we knew everything about the machine except the starting point in its cycle of operation, then a set of characters specifying the starting point would constitute the key.

These concepts can be illustrated by an example which is in itself of considerable interest. The machine about to be described

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

is a somewhat simplified version of the [redacted] The simplifications adopted make description and enumeration of configurations easier, by avoiding certain actual details. The sizes of the various exhaustion problem are somewhat altered by these simplifications, but the alterations are not important. The simplified [redacted]

English text uses 27 characters counting spaces, and thus there are 27^m sequences of m characters. Shannon's results indicate that only about 2^m of these make "good English," and if these make up less than $1\,(2 \times 10^{541})$ of the whole there will ordinarily be only one of the 2×10^{541} starting points which will convert our message to good English. This is the condition we must meet if we are to successfully decrypt the message by exhaustion, for we must recognize the correct message as the only reasonable possibility among 2×10^{541} attempted decipherments.

The condition

$$(2^m)\ (2 \times 10^{541})\ \leq\ (27^m)$$

leads [redacted]

Suppose a calculating machine, equipped with a full knowledge of the subtelties of English, were to try all 2×10^{541} starting points. It would not need to carry all trials out for many characters. The average trial length might be, say, 20 characters, with a minimum energy requirement per character tried of, say, 10^{-23} kilowatt hours (see Section 2 of the Supplement to this Appendix for details). The total energy required would then be 2×10^{520} kilowatt hours. This amount is quite fantastic, so fantastic that meaningful expressions are impossible. For example, according to modern physical theories, it is many times the total energy in the universe.

Thus, although the problem is in principle soluble by this simple technique, there is fundamentally no possibility at all of carrying out such a program.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Cryptanalysis proceeds (when it proceeds at all) by splitting the problem into smaller ones which can be attacked by hand or by machines of reasonable speed. It is the cryptographers' purpose to design a machine and to devise and enforce a regimen for its use such that the problem cannot be split and is thus unassailable. It is the cryptanalysts' purpose to acquire small pieces of information about a complex machine by its improper operation or employment [redacted] in order to make possible the reading ("exploitation") of the encrypted messages.

Thus, it is a simple matter to recognize [redacted]

[redacted] at present prices. This is still far in the range of the fantastic, yet success would provide only one setting, thus allowing us to read one specific message and greatly facilitating reading other messages sent over the same link on the same day. Even with full knowledge of the rotor box, straight exhaustion is not practical.

In either of these examples, the prospect would have been gloomier had we assumed, not the use of all the statistical structure of text which Shannon's work indicates, but instead only the use of single letter frequencies, letter pair frequencies, etc. Instead of a redundancy of 4 bits per character, we should have been able to use only 1 or 2 bits of redundancy per character. This would have multiplied our computing labors by a factor of from 4 to 2. In comparison with the large factors actually present, such a factor is nearly negligible, and might indeed be entirely compensated for by increased ease of recognition of structure. (It would, of course, call for 2 to 4 times as long a message, but the standard practice of subjecting to refined examination only those trials with satisfactory simple statistics would allow us to take advantage of the gain in ease of recognition without requiring longer messages.)

Should a [redacted]

starting points to try. Fifty thousand million million trials is still many, but the scale of this computing problem can now be contemplated. With 1960 equipment, this should tie up about a hundred million dollars of computing machine for a week. (See Section 3 of the Supplement to this Appendix.) Even this, far simpler, problem had better be done in some way other than simple exhaustion. (There is no substitute for ingenuity in modern cryptanalysis.)

In the foregoing calculations we have considered the minimal length of message essential for decryption. A further possibility is provided by the use of elements of messages of more than a minimum length. To exemplify this, suppose that we are using a redundancy of 1 bit per character and at that rate that a theoretical minimum message length of 500 characters is required for decryption. This means that the method of exhaustive trial would require us to examine 2^{500} cases to find the proper plain text. On the other hand, if we intercept a message 501 characters long we have one excess bit of information at our disposal. Naively, one might hope that this would mean that we could find the correct message by searching among only 2^{499} alternatives, and so on. Thus, one would hope that by intercepting a message about a thousand characters long he could so limit the problem that it would be computationally manageable.

It is quite possible that there is a basic difficulty here, as would be the case were it a mathematical fact that there is no easy way of using the extra information to categorize the given possibilities, without requiring an amount of computation comparable with that we are trying to avoid. This question falls in a still unexplored mathematical area. Current study of theorems which may tell us whether certain sorts of encryption are basically more effective (can use fewer computer operations) than the corresponding decryption may help to clarify the situation. (Such work is in progress at AFCRC by Professor Gleason of Harvard University, a member of this panel.) This question, and the problem of stating what we mean by high-order language statistics, or of a low order of low-order statistics, illustrate some of the basic theoretical areas which are still unexplored.

While information theory provides a firm and useful basis for cryptanalytic studies, much work must proceed from a more particular point of view. We have seen in the foregoing example a coupling of information theoretic ideas with the constraints of a particular machine structure. Other possible structures in the process of encryption can, however, be assumed and investigated.

At Air Force Cambridge Research Center a small group in the Communications Laboratory is studying "cryptographic systems for non-literal data." The group developed from some IFF studies some years ago. They have contact with, but, they claim, small fertilization from, NSA. They have decided to put their main (small) effort on theoretical research directed at complete understanding of a few <u>simple</u> systems; viz., N to N mappings. They have initiated a series of summer studies, like SCAMP, and will perhaps continue some small individual contracts through the windows. The summer studies are presently conducted at Brandeis University at a level of about $50,000 per year. The main task is to investigate the structure of groups with two generators, etc., and to consider a list of specific problems. The director of the current summer study is A. A. Albert; other participants include Mills and Herstein from Yale, Shaeffer from University of Connecticut, Lowell Page, Kaplansky, and half a dozen others. It clearly resembles SCAMP strongly, and was doubtless modeled after it. Its advantage is that its problem field is not nearly so extensive and ambitious.

In summary, we conclude that information theory provides an attractive, promising, and one might hope, a fertile setting for the cultivation of cryptanalysis. It can be employed in connection with the study of systems for encryption of voice or picture signals as well as in connection with text; the broad principles involved are the same.

Together with this broad view, however, we need both particular data and a degree of specialization. We need some explicit statements concerning the redundancy of text and other signals, rather than mere estimates of the amount of redundancy. We need ways of detecting statistical structure.* We need a clear formulation of cryptanalytic procedures, as discussed in Appendix IV,

---

* This problem is commented on in Technical Supplement II, "Recognition of Complex Logical Structure by Audio or Visual Means"

"Programming Methods." We need a degree of specialization such as that provided by a given type of machine or a given sort of transformation. All of this can be provided only by research of the broadest and most fundamental kind.

SUPPLEMENT TO APPENDIX II

1. <u>Calculation of number of machine structures and initial positions</u>.

A 47-point rotor is wired to connect each of 47 given points to one of a second set of 47. In a given position this can be done in

$$47! = 2.59 \times 10^{59}$$

ways. (If the same rotor in different positions is regarded as equivalent, there will be $47!/47 = 46! = 5.50 \times 10^{57}$ different rotors.) A 47-point hot plate with 23 or 24 points hot or a 47-point ring with 23 notches can be arranged in

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

$$\begin{bmatrix}47\\23\end{bmatrix} = \frac{47!}{23!\,24!} = 1.61 \times 10^{13}$$

ways. A machine made up of a number of such elements, each of which may be chosen separately, has a number of possible configurations (combinations of structures, arrangements and settings) equal to the product of factors, one for each element, where each factor is equal to the number of configurations for that element.

[redacted]

At the other extreme, if the selections and arrangements of rotors and notch rings are known, as is the wiring of the hot plate, then there remains only the setting to be determined. If only the 8 rotors are to be set, there will be only

$$(47)^8 = 2.38 \times 10^{13} \text{ possibilities.}$$

If the 4 notch rings are also to be set, there will be 12 settings in all, yielding

$$(47)^{12} = 1.16 \times 10^{20} \text{ possibilities.}$$

If only the 6 movable rotors and the 4 notch rings are set, there will be

$$(47)^{10} = 5.26 \times 10^{16} \text{ possibilities.}$$

It is this last value which appears in our example in Appendix II.

In the intermediate situation, where the 'rotor box' is known, we obtain an intermediate result. If there are 12 rotors in the rotor box and 8 are to be used in the machine, then there are

$$\frac{12!}{4!} = 1.00 \times 10^7$$

ways of assembling rotors. If there are 14 notch rings, and 4 are to be used in the machine, then there are

$$\frac{14!}{10!} = 20,020 = 2 \times 10^4$$

ways of selecting and placing notch rings. The hot plate can, as noted above, be wired in

$$\frac{47!}{24!\,23!} = 1.61 \times 10^{13}$$

ways. Including settings, there will be, in all

$$\left[\frac{12!}{4!}\right] \left[\frac{14!}{10!}\right] \left[\frac{47!}{24!\,23!}\right] (47)^{12} = 3.74 \times 10^{44}$$

configurations.

2. <u>Power requirements for exhaustion attacks</u>.

Perhaps the simplest and most invulnerable way of showing that certain attacks by complete exhaustion are fantastically impossible is by calculating a lower bound for the power required. Present computers use very much more power than this lower bound suggests, and it is probable that, even with the improvements which now appear [redacted] to ten years, actual power requirements will be 10 million times those given by the lower bound.

In a simple exhaustion attack, proceeding character by character, the following operations have to be carried out in connection with each character: recognition of the character, reference to simulated configuration of the machine, calculation of 'deciphered' character, advance of simulated configuration. It does not seem possible to do this with appreciably less than 100 binary choices, whose results must be recorded, at least temporarily.

Each record of a binary choice must be reliable, and consequently must involve an energy change large compared to random thermal fluctuations. The energy change typifying such fluctuations is $kT = 4 \times 10^{-14}$ ergs $= 4 \times 10^{-24}$ kwsecs $= 10^{-27}$ kilowatt hours at room temperature. (Even if the computing elements are refrigerated, the heat transferred at room temperature will have to be related to this amount.) If a record of a binary choice must amount to a minimum of, say, $100\ kT = 10^{-25}$ kilowatt hours, then a single character, with its 100 choices to be recorded, will require 10^{-23} kilowatt hours. This is the figure used as a lower bound in the body of this Appendix.

3. <u>Speeds, power requirements, and costs probably achievable in the near future</u>.

Estimates of speeds, power requirements and costs of super-high speed computing equipment possible in the next ten years can only be rough. The figures given in Table A are believed to be reasonable.

In order to bring these figures into a usable form we need to introduce (i) the cost of electric power, which we shall take as one cent per kilowatt hour, (ii) the investment required to generate electric power, which we shall take as $300 per kilowatt of capacity, and (iii) the fraction of the memory being consulted at one instant, which we shall take as 0.01. Using factors (i) and (ii), the numbers in Table A lead to the following estimates (for apparently useful systems)

		Bits possibly handled per week for each million dollars spent on		
System	Status	Computer	Generators	Power for a year
1960 - Transistor	Building	6×10^{16}	10^{21}	4×10^{21}
1965 - Transistor	Possible(?)	2×10^{19}	2×10^{22}	8×10^{22}
1965 - Cryotron	Perhaps	6×10^{22}	2×10^{24}	8×10^{24}

Per million dollars of investment, the numbers of characters handled per week in an exhaustion attack would then be roughly as follows, when we make allowance for the fact that only one

one-hundredth of the memory is likely to be used on any cycle.

1960 - Transistor	6×10^{14}
1965 - Transistor(?)	2×10^{17}
1965 - Cryotron(??)	1.5×10^{22}

TABLE A

Date	Memory System	Cost/bit (installed)	Energy/bit	Repetition Rate	Bits/year per million dollar investment
~ 1960	Transistor (stretch)	\$100	2×10^{-2} erg	10^{7}/second	3×10^{18}
~ 1965	Transistor (*)	\$1	~ 10^{-3} erg	3×10^{7}/second	10^{21}
~ 1965	Cryotron (**)	0.1¢ (***)	~ 10^{-5} erg	10^{8}/second	3×10^{24}
~ 1965	Optical (**)	10^{-4}¢ (****)	???	10^{2}/second	3×10^{21}

* Assuming an all-out effort on an all-parallel machine, this <u>may</u> be possible.

** Also quite problematical.

*** Assuming so far unknown fabrication techniques.

**** 10^{8} bits/plane at \$100/plane.

APPENDIX III

BULK TRAFFIC INTERCEPT AND HANDLING

(b)(3)-P.L. 86-36
(b)(1)

We have noted in the body of the report that the global operations involving some [redacted] people needed to man, to service, and to harvest the [redacted] accounts for the primary expense of the communications intelligence job. The tremendous flow of material so harvested into NSA headquarters at present sorely taxes a staff of 10,000. Largely because of the necessity of transcribing incoming material into a suitable form, serious backlogs have repeatedly arisen either in the processing of material or in the availability of material for cryptanalysis or traffic analysis.

Clearly, a more rational approach to the proper sampling of [redacted] is necessary in keeping the material intercepted and processed within reasonable bounds, and this matter has been discussed in the body of the report. However, the amount of material which can be reasonably intercepted and processed depends on the intercept and processing methods used.

While the bulk of present traffic seems overwhelming when measured in reels of paper and magnetic tape and tons of hard copy, it is not necessarily unmanageable when considered in terms of the speed of modern electronic computing machines. For instance the

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted] computer is capable of reading from magnetic tape at a rate of 90,000 bits (binary units) of information (pulses) a second. According to our estimates, this is a few times faster than the total input of COMINT material to the NSA. Moreover, fast printers such as the [redacted] can print out hard copy from magnetic tape at a rate of 2,000 characters a second, corresponding to 10,000 bits a second. Thus, if all the traffic were to arrive on the proper sort of magnetic tape, a considerable portion of it could be turned into hard copy (page print) by a few fast printing machines (if this were useful or desired).

These preliminary remarks have been made chiefly to indicate that it is within the scope of the present art to design electronic machines which could cope with the entire input of material to the NSA, if only that material arrived in a suitable form and if proper use were made of available modern methods of data handling and processing.

What is called for in traffic intercept handling is a well-thought-out program for mechanizing and expediting all phases of the handling of traffic in bulk, in order that the personnel employed may as much as possible be employed at tasks requiring their powers of human judgment.

One important problem for instance is the mechanization of [redacted] The NSA, recognizing that about 70 per cent of all the [redacted] including even military where many copies are required),

(b)(3)-P.L. 86-36
(b)(1)

has already designed schemes expected to be in the field by June, 1961, which will take down these [redacted] with least manpower. It was estimated that perhaps [redacted] by mechanical replacement in this area. Undecided issues include, however, whether or not the reception should be directly translated in the field to some punched tape or other machine-accessible form, in which a rapid mechanical word-recognition survey could be done. Our later discussions of plain-text processing will return to this issue.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

It is estimated now that as much as 80 per cent of operators' time in the field may be spent sitting waiting for a signal to come. The possibility that an operator could monitor a fairly broad band-width by use of a broad-band receiver should be explored. The question of how much could be covered by a band-pass filter without specific tuning should be answered.

It should be possible to improve the quality of the large volume of automatic interception by better receiving antennas. An antenna study is emphasized in sections on the research and development program. [redacted], even for routine communication, it is important to have adequate quality of reception for traffic analysis and identification.

Because all the NSA's activities depend on the accurate interception of signals, NSA should exercise a strong technical leadership in receiver problems, and in the problem of ascertaining and recording very accurately the time of reception of signals as a means of signal identification as well as of proper logging. Through its technical strength, the NSA could be of considerable help to the services in this field.

Where operators or occasional operator intervention continue to be necessary, the identification of unusual or weak signal type should be supported by an up-to-date "electric dictionary" for spotting of items whose significance is indicated by other sources.

The importance of recording COMINT material in proper form at the intercept stations cannot be overemphasized. At present, some traffic is recorded in audio form on magnetic tape. This is relatively bulky and costly, but it has advantages. In the case of weak signals which result in garbles (mistaken interpretations of characters), which are very serious in cryptanalysis, audio recording preserves the signal together with the noise or interference in its original form, so that sophisticated means can be used to distinguish the signal from the noise. Further, audio recording is adaptable to signals of all sorts, including new types of signals.

Thus, we believe that intercept stations should be equipped with adequate audio recording facilities to handle weak signals and a fair volume of traffic of new types, should they appear.

It is advantageous in many ways to transcribe the signal into a digital or on-off form and record it on magnetic tape, and the NSA has done good but insufficient work toward this end. The

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

advantages of such recording are that it is less bulky than audio recording and that it can be read more quickly and certainly by electronic machines. As indicated, the disadvantages are that devices for transcribing signals digitally handle only one system or one type of system, and that if they make a mistake on a weak signal there is no way of reprocessing the data as in the case of audio recording.

Sometimes hard copy is made at intercept points. While hard copy may be made for immediate tactical use, hard copy should never be the only transcript of a received signal. All received signals should be recorded on magnetic tape so that they can be sent electromagnetically and automatically to processing centers, and so that they can be read by machines. Even signals typed out by a listening operator could readily be transcribed to tape at the same time if a suitable machine were used.

At present, a good deal of punched paper tape is used in NSA operations. Compared with magnetic tape, paper tape is slow and bulky, and its use must prove expensive in the long run. Every effort should be made to do all recording on magnetic tape in a uniform manner.

If a wise sampling of traffic is to be made, it is important to exercise as much jugment as is soundly possible in the field. If [redacted] or faulty transmissions, then it is important that traffic containing

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted] be selected and forwarded to the Agency promptly. NSA has done work on [redacted] for use in the field, and a field trial is under way. This is a step in the right direction, and the matter should be pressed vigorously.

Tactical considerations make it most desirable that recognizably relevant material be sorted out near or at the point of intercept and made immediately available for local tactical use. It is equally necessary to sort material as to its urgency of transmission, so that limited facilities for electromagnetic transmission to NSA headquarters will be as efficiently used as possible. This latter operation can only be effectively carried out by persons of high competence. The shortage of such persons makes extreme decentralization of this latter task impossible.

The final stages of field processing cannot be effectively decentralized and certain other stages should not be. The NSA has already recognized the advantages of concentrating field-processing operations at a few points. (Indeed it has considered one processing center in [redacted]) A trend in this direction is inevitable and should not be blocked. Some care may be required, however, to protect the requirements of tactical commanders. Hard copy of manually transcribed messages can be furnished locally, either by carbon copy, as at present, or, in the future, in parallel with the magnetic tape for further processing. To this possibility there may need to be added a word-recognition machine capability for local use, and, conceivably, machines for decryption of [redacted]

Far more important, however, is the provision of a better communications net among the intercept and processing stations in an extended area. All or almost all COMINT material could then be transmitted directly to the major processing centers by electromagnetic means; there it could be sorted, analyzed, and either supplied to users, transmitted to NSA headquarters electromagnetically, flown to NSA headquarters, or discarded.

Any such field processing centers should be operated directly by NSA because only NSA has the experience and competent personnel to do the job efficiently.

In forwarding intercept to processing stations, strong and familiar signals can be sent and transcribed by digital means. Unfamiliar signals can be sent from audio tapes. For this purpose some method of encrypting audio signals is needed. In the case of weak signals, audio tapes can be flown to the processing centers for comparison with digital tapes.

After some sorting or processing in the field, urgent material can be sent to NSA headquarters electromagnetically in digital form. Less urgent material can be flown to headquarters in the form of digital or audio tape. An effort should be made to avoid ever shipping hard copy. Fast printers should provide transription from magnetic tape to hard copy virtually without delay, and so make the shipping of hard copy unnecessary.

There should be a great increase in the use of fast electronic machinery in data-handling functions both in field processing centers and at NSA headquarters.

Electronic machines could be used to sort and retranscribe routine messages according to callsigns or standardized headings. They could perhaps perform certain editing functions in reproducing such messages in a desirable format. The NSA has begun to consider such problems, but it is urgent that more be done about them.

Electronic devices could look in messages for key words or phrases. They could sort and transcribe messages on this basis. Again this has been considered,* but it has not been adequately implemented.

Much if not all routine decryption could be done by electronic machines. Some decryption [redacted] is being done in this way, and machine methods are used as a tool by cryptanalysts, but machine decryption should be extended and mechanized, as discussed elsewhere.

At present, the NSA has considered the problems discussed above, and it has often considered them intelligently and thoughtfully. It has not done enough abou them, however. Something more is needed.

Partly, what is needed is a careful analysis of the real problems of bulk traffic intercept and handling, to see what can be done now and what should be done in the future. The traffic handling activities of the NSA should be organized and equipped accordingly.

Partly, what is needed is vigorous research and development aimed directly at overcoming problems of traffic intercept and handling and making them faster, more flexible, and cheaper.

---

*Technical Supplement III discusses one way of doing this.

APPENDIX IV

PROGRAMMING METHODS

A major problem connected with the use of modern large-scale computing and data-processing machinery is that of programming, the process of translating instructions from the language used by people to the language used by the machine. The modern stored-program machine is a truly universal device in that it can, in principle, solve any problem that can be solved by any machine. There are two obstacles, however, and either may make it impractical to solve a particular problem at a particular time on a particular machine. One of these is obvious. It is cost, either in dollars or hours. A particular problem might be too large for either budget or patience. The other is that among problems that are small enough, there are some that are too hard to state to the machine. A problem may require too many man-hours of too high a calibre of programmer to translate the statement of the problem into machine language. This appendix is concerned with these problems which are now too hard to state. It recommends a course of action to alleviate the difficulty.

In the course of the Panel's work, it has considered the problem of exploiting [redacted] The evidence indicates that more sophisticated automatic programming methods would be of great value for handling these [redacted]

Automatic programming is a method of getting the machine to help the programmer translate the instructions from English (and mathematical symbols and specialized terminology) into machine language. The method is to devise an intermediate language which has two properties:

1. It is easier for a person to translate from English, etc., to the intermediate language than to machine language.
2. It is possible to write a program to enable the machine to translate from the intermediate language to its own language.

In the NSA there have been some important automatic programming achievements, and there are now some commendable projects under way. However, the NSA, by the nature of its work, is faced with an extraordinary problem that seems to have inhibited the fullest development of automatic programming methods. The work of the NSA has required the acquisition of a great variety of automatic calculators. A major unsolved problem in automatic programming is how to translate mechanically from one machine language to another, or even how to get an intermediate language that would be suitable for all or at least many automatic calculators.

A comprehensive automatic programming project for the Agency would indeed require solution of this currently unsolved problem. But, on the other hand, too many inspired creative programmers would be required to prepare separate automatic programming systems for each type of machine. This situation seems to have dissipated some of the Agency's strength in the development of automatic programming methods, as will be seen below.

In attacking a production problem it is necessary to use only methods that are quite sure to be relevant and quite sure to work. The development of new methods and their refinement to the point at which they can be picked up by the PROD area of NSA is a proper function of its R/D area. To state this in another way, sometimes a method is well enough understood so that there is a reasonable chance of success in applying it to a current problem. When this is true it should be the task of PROD to carry out the programming. At other times, a promising method may be so new that it can be applied effectively only to simplified problems or problems that are no longer current. The hope would be that, after successful application of the method to a simplified problem or to a graded succession of simplified problems, the method would be well enough understood so that it could be applied to current problems. This longer-range approach is a proper function of R/D, and while there are now commendable efforts of this sort, the Panel recommends even more emphasis in this direction.

There seem to be three useful approaches to programming research in cryptanalysis. One of these is the development of intermediate languages, as mentioned above. The NSA now has two research contracts that are aimed at this problem. One of these, with Allan Perlis at Carnegie Tech, is aimed at the problem of the multiplicity of machines. The research is aimed at the production of an intermediate language and an array of translation programs, so that one can write a program in the intermediate language and then translate it to any of several machine languages. To our knowledge, no such comprehensive "universal language" has so far been written. If the project is successful it will be an important step forward.

The other contract is with L. Roberts of General Kinetics. The project is to produce a language for cryptanalysis which, hopefully, could in turn be translated by machine into machine language. This would be an important step, and it should, if possible, be made. Only because most branches of mathematics are so well reduced to a tidy language has it been possible to produce such powerful automatic programming methods as are now available for many parts of mathematics. If cryptanalysis can now be pushed as far along this route as mathematics has moved (during many centuries), real automatic programming of cryptanalysis will be much easier to achieve.

There exists a grand concept: it should be possible to combine these two programming advances now being sought by stating the cryptanalytic language of Roberts in the universal language of Perlis. The Agency would then be able to give its cryptanalysts the means to use the large machines without becoming programmers and without having to operate through programmers who do not, by and large, understand cryptanalysis. While the Panel endorses this grand objective, it is concerned that there are apparently no plans to use the cryptanalytic language sought in the Roberts program unless (or until, or to the extent that) the Perlis effort is successful.

It does seem that a strong effort is needed to produce a cryptanalytic equivalent of FORTRAN, which has done such a large job in the application of machine computation to a wide variety of analytical problems. However, FORTRAN required 27 man-years of effort by a close-knit team of highly capable people who were directed by a very talented leader. The Agency is tackling a much more difficult problem, in that the language of cryptanalysis is not yet as tidy as mathematics, and in that a common language for many different machines is sought. Yet, this much more difficult objective is being pursued by two groups, loosely coordinated because of contractual relations, geography, and the requirements of security, and totaling far fewer people than were necessary to develop FORTRAN.

The Panel recommends that effort along these lines be reenforced, to the end of obtaining some useful result in a reasonable time.

Squarely in the way of machine methods of cryptanalysis stands the fact that expert cryptanalysts cannot explain clearly how they do their best work. Before machine methods can duplicate their results, someone must find out just what they are doing. Here the best course seems to be to seek machine solutions of

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

simplified problems or of real problems of yesterday. Such a course could be an important way to develop the theory and understanding of automatic machine cryptanalysis, so that some day it will have grown to the stature of today's big problems. The recent successes of the [redacted] is an example of the kind of effort needed here.

When a task has been performed by a machine, one usually has a much clearer understanding of it than could be obtained solely through human ingenuity, intuition, and imagination. It is common experience among programmers that if one thinks he understands a process and then writes a program to make a machine do it, he attains a much more profound understanding of the process. The act of programming appears to subject the programmer's understanding to the scrutiny of some kind of a "logical microscope" that detects many subtleties which are not evidence to the naked eye.

In summary, there are two advantages to research on automatic machine cryptanalysis on simplified or small problems. One is that the activity develops the art so that it may come within range of the big problems, and the other is that the very act of such programming will reveal things about cryptanalysis.

The third approach to the cryptanalytic programming problem is revealed by recent programming developments in other areas. It has recently been shown* that programs can be written to enable a

---

* "The Logic Theory Machine," H. A. Simon and A. Newell, in Trans. IRE Prof. Group on Information Theory, September, 1956

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

computer to exhibit ingenuity to prove theorems. Further work in this area is proceeding at the Carnegie Institute of Technology, the Massachusetts Institute of Technology, at International Business Machines Corporation, and elsewhere. It appears that there may be a very close relation between this theorem-proving type of program and programs that could be used [redacted] The essential step that is performed in the theorem-proving program is that the machine makes shrewd guesses that it later tests and by so doing is able to prove theorems that would take much too long, sometimes even an infinite period, to prove by the conventional slow, plodding, systematic programs. The cryptanalytic parallel is that by guessing at a crib and then checking, one is sometimes able to solve a problem by hand faster than a high-speed machine can do it exhaustively. If these new methods of programming can be made to allow the high-speed machine to use guesswork efficiently, a great increase in speed may be possible.

In summary, advances in programming, unlike improvements in machine technology, are always immediately available for application both to current problems and to advance the science of programming. Thus there should properly be an extremely rapid progress in the production and improvement of automatic cryptanalytic programs just as has been the case in programs for mathematical computing.

Recommendations

The Panel recommends that the Agency increase its effort in programming research by:

1. Seeking, in addition to its present programming undertakings, a more direct route to a cryptanalytic equivalent of FORTRAN.
2. Placing more emphasis on the development of automatic machine methods for simplified problems and old problems as a part of an orderly development of cryptanalytic theory.
3. Investigating the possibility that methods resembling the new machine theorem-proving methods will be useful in cryptanalysis.

TECHNICAL ADJUNCT I

THE POSSIBLE ROLE OF AUDIO AND VISUAL RECOGNITION

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

1. The general situation.

Information theory tells us that much statistical structure must persist in a verbal message encoded with a limited key, e.g., by [redacted] This structure is not simple, the art of the cryptographer has been used to destroy all simple structure and many not-so-simple structures. One of the arts of the cryptologist has been the deep and refined study of machine systems in the hope, formerly with encouraging successes, of finding not-so-simple but not-too-complex structures which would reveal significant information about the machine or its settings. Unrandomly frequent repeats at interesting and significant distances, the use of window indexes, etc., are examples.

If we are to make real use against [redacted] use of the statistical structure which information theory assures us must be there, we will probably have to deal with not-so-simple statistical patterns. Two main difficulties stand in our way. First, difficulties of calculating individual measures of individual sorts of not-so-simple patterns. Second, once we consider not-so-simple structures the multiplicity of possible structures we must consider rises rapidly. Both of these factors combine to present a difficult computing load, but computer speed and logical flexibility continue to improve.

Devices using human recognition offer certain relatively unique opportunities when we wish to look for not-so-simple structures. Two basic considerations operate here; (i) a human can listen to, but more especially look at a very considerable body of information "at once," and (ii) a human will often detect structure in a sound or visual pattern without advance knowledge of what pattern might be present. It is this latter feature that is crucial. Once we know that we are looking for one of a few types of pattern, a machine can almost always be made more sensitive than a man.

The human brain, when supplied through its best information channels (the optic nerves) is much the most subtly flexible data-processing system we know for complex situations. The problem of using it effectively is one of presentation.

2. Examples.

Some examples may make the situation clearer. To begin with what we are trying to find is some logical structure in a nearly random function, like random noise, or a random ray. If we consider in particular the acoustics problem we notice that random noise has a flat power spectrum. So also does an impulsive noise like a pistol shot. The difference between a pistol shot and thermal noise is, however, immediately recognizable to the ear. The characteristics of the pistol shot are of course carried by the phase spectrum and could be discovered if the phase spectrum were computed. We would, however, not normally do this, unless we were expecting something like a pistol shot, and in any case the problem of recognizing the existence of a pistol shot from the phase spectrum, particularly if it were largely masked by accompanied random noise, might be difficult. Similarly the ear would have no difficulty in recognizing also more complex structures, such as a pistol shot with reverberation. The same considerations apply to the eye. A flat amplitude spectrum might represent a random time function. It might also represent a peaked standing wave, if the phase spectrum were just right. There would be no difficulty here in picking out such variations from this as a wave with reflections or a wave moving relatively slowly in one direction.

Optical displays have the advantage that they can directly exhibit relations in two dimensions. We may visualize in particular an oscilloscope display such as that furnished by a television screen. By permitting the input to vary continuously with a third parameter, and relying on memory, one might, to a limited extent, be able to display logical situations involving three parameters.

It appears from the discussion in the section on information theory that the ideal encoded message has all the characteristics of random noise. Thus a visual display of the sort described prepared in any normal manner should appear as a slightly mottled structureless gray. Any suggestion of a more definite pattern than this would represent a hint of a logical structure worth inquiring into further. One need only think of the infinite diversity of fabric patterns on wallpaper or the distortions of such patterns which preserve structure but destroy strictly periodic properties to realize how much better the eye would be in perceiving such systematic, but unpredictable, relationships than any possible machine.

We must, of course, expect to deceive ourselves many times, since the most we can hope for is a faint pattern superimposed on a strong random background. But it is not necessary for the recognition to be infallible. We can cheerfully follow many false trails if the reward is to have discovered a few real clues.

3. Nature of displays.

Cryptanalysis has long made use of such abilities of eye and brain in an elementary way. Writing out cipher text "on a width of" one or more selected numbers is a classical technique -- a technique adapted to visual perception as well as column statistics. But most, if not all, applications to date have presented characters. The present discussion has tacitly assumed that the presentation would be in shades of light and dark, by various colors, or both. On the other hand, it does not attempt to say, beyond this, exactly what would be displayed on the screen. The proper choice of function and parameters to be utilized is the principal part of the problem and would best be undertaken from a background of deep understanding in cryptanalysis. Presumably, however, the display would not be prepared directly from the message itself, but from some simple statistics computed from the message. For example, in a literal message one might even use as a basis the "autocorrelation" functions computed from the time series obtained by replacing a given character by 1 and all other characters by 0. Higher-order correlations of the same sort involving more than one letter will readily suggest themselves. Such computations would describe mathematically many of the simple statistics of letter occurrence, particularly in the presence of [redacted]

The preparation of the material for such displays would evidently require a large amount of computing of a rather elementary sort. Since the outputs are probably simple correlations independent of any time reference, the use of computers involving a very large number of elementary parallel modes, as suggested in Appendix suggests itself.

4. Operational experience.

There is a precedent for such displays in visible speech and in visual means of underwater sound detection. To persons familiar with these fields the startling power of the eye in picking out an elaborate pattern in the presence of a diffuse background is an old story. In underwater sound detection, for example, the eye provides an additional integrating means, aside from that provided by the ordinary filtering in a sound spectrograph, which permits a very low-level signal to be detected in the presence of a high-noise background. Moreover, the patterns can be found not only for stationary vessels, with fixed signal frequency, but for vessels moving in complex ways, so that the patterns vary gradually with time. The situation in visible speech is still more striking. Here the instantaneous patterns are themselves complex and follow one another with great rapidity. The fact that we can visually detect and read such a jumble is startling evidence that the eye provides a more intimate link between the brain and complex structure than we have been able to obtain to date through any resort to formal mechanized processes. (Though once a particular structure has been recognized, mechanical detection may be more sensitive.)

TECHNICAL APPENDIX II

SOME METHODS OF RECOGNIZING WORDS

AND OTHER SYMBOL GROUPS

(b)(3)-P.L. 86-36

While the NSA has given some attention to the development and use of automatic word recognizers, present-day technology offers possibilities which do not seem to have been fully exploited. The possibilities which follow are presented both on their own account, and as illustrative examples. For convenience and simplicity they assume input from a six-channel magnetic tape, such as that used in an [redacted] data processing machine. The techniques are, however, applicable to any digit input.

1. Utilization of the principle of the 'Diamond Ring Translator,' a standard telephone exchange component.

The general scheme is indicated in Fig. 1. The characters are fed from the tape into a shift register. If the characters are 6-bit characters as indicated, 6 bits may be fed in simultaneously. Either 6 parallel shift registers may be used, or the bits may be arranged in serial form. When a new character is fed in, either the 6 parallel shift registers each advance one position or, if one serial register is used, the register advances six positions. As outputs from the registers, there are available some M pairs of leads corresponding to the M total bits in all of the characters of the longest word whose presence can be recognized by the device. For a given bit, an approximately constant voltage output on the

1 lead with no voltage output on the 0 lead indicates 0, while an approximately constant voltage output on the 0 lead with no output voltage on the 1 lead indicates 1.

The various bit leads are led to a plugboard which is internally wired so as to recognize or respond to words of a given vocabulary. This plugboard will have P outlet leads, where P is the largest number of words which can be recognized by means of the plugboard. Each output lead goes to a box marked output circuitry. Signals on leads from this box indicate the presence of a word in the vocabulary or in some sub-group of the vocabulary.

Figure 2 indicates one possible nature of the plugboard, which is very similar to the Diamond Ring Translator used in telephone switching. Each pair of digit wires is threaded through a set of pairs of magnetic cores, which are shown in cross section in the drawing. A pulse on a 0 lead will induce a negative voltage in any wire threading the "0" core to which it is connected, and a pulse on a 1 lead will induce a negative voltage on any wire threading the "1" core to which it is connected.

Two wires are shown threading the cores. The wire labeled 0100 so threads the cores that when the signal from the shift register is 0100 reading from bottom to top, the 0100 lead threads no excited cores and no voltage will be induced on it. We will remember that the absence of a pulse on a lead indicates 1. For any other threading of all 4 cores, a wire would have a negative voltage induced on it.

At the time at which the voltages applied by the shift register are at their maxima, a small positive reading pulse is applied along the wires threading the cores by means of the reading pulse generator PR. If a wire to which the pulse is applied threads no active cores, this pulse will cause current to flow through a series diode D_s and to an output lead OL. For instance, if the voltages from the shift register signfy 0100, the output pulse will cause current to flow through diode D_{s1} to output lead OL1 of Fig. 2.

Because transformers can transmit ac only, positive voltages in the wires threading the cores will follow the negative voltages produced by pulses from the shift register. These positive voltages cannot produce output at the output leads OL because of parallel-connected diodes D_p. An output lead can go positive only when the reading pulse is applied to the parallel diode D_p, as well as to the wire connected to the corresponding series diode.

Sometimes we may wish to get an output corresponding to a short word. In this case we thread the wire through only some of the sets of cores. For instance, in Fig. 2 wire X011 will give an output when the shift-register supplies signals corresponding to either 1011 or 0011 to the plugboard.

Various output leads can be connected together to give a combined output for a particular section of the vocabulary, or all output leads can be connected together to give a response when any word in the vocabulary is read out of the shift register.

It is possible that the capacitances of the diodes driven negative will cause an appreciable signal when many output leads are connected together. This can be guarded against by replacing the series diodes by the configuration of Fig. 3, retaining the previous parallel diodes, which are not shown in Figures 3 and 4.

If we replace the series diodes by the configuration of Fig. 4 we can avoid applying large negative voltages to the series diodes.

It may be desirable to make the output associated with a given portion of the vocabulary available in binary coded form. This can be done by threading an output wire through a series of cores, as shown in Fig. 5. Here an output pulse on wire W_1 produces pulses on leads corresponding to the number 010, reading upward, while a pulse through wire W_2 produces an output 110.

It is worth noting that a "word space" is a character, so that it will be possible, and may or may not be desirable, to define a word as consisting of certain specified characters preceded, or followed, or both proceeded and followed, by a word space.

As the above scheme has been outlined, 6-bit characters might be read in every 1/15,000 second, that is, every 67 microseconds. If parallel shift registers were used and the bits were read in parallel, no operations would have to take place more frequently than this. In order to induce sufficient voltages in the leads, which thread a given core but once, it would probably be desirable that the length of the pulses supplied from the shift register be held down to about one microsecond. One might also apply the pulses from the shift register to, say, a 10-turn primary, so that 20 volts at a comparatively low current applied to a core by the shift register would produce 2 volts in a wire threading the core.

We may note that to accommodate 5000 5-mil wires, the cores would have to have openings with diameters of around a half an inch.

In order to make it easy to thread the cores, U-shaped sections could be mounted on one support and threaded; then, the magnetic circuits could be completed by bar-shaped sections mounted on another support.

2. A core-memory device.

Figure 6 shows another sort of word recognizer in which cores are used not as transformers but as magnetic storage devices. Here there are two columns of cores and the digit pulses from the shift register are currents to the cores; a current to a 0 lead for a zero and to a 1 lead for a one. Currents in the 0 lead set cores in column 1 opposite from cores in column 2, and currents in the 1 lead set cores in the opposite sense from currents in the 0 lead. After the cores are set by a given set of digit currents from the shift register, a reading voltage is applied to wires threading the cores. If one of the wires so threads the cores that the reading voltage tries to set all the cores along its path in the same sense in which the digit pulses have already set them, then an appreciable current will flow into the low impedance load and an indication of recognition will be obtained by means of the amplifier A. If no wire is so threaded through the cores as to tend to set them in the same direction in which they had been set by the digit pulses, then the reading pulse voltage will cause no appreciable current through any of the wires and no indication of recognition will be obtained.

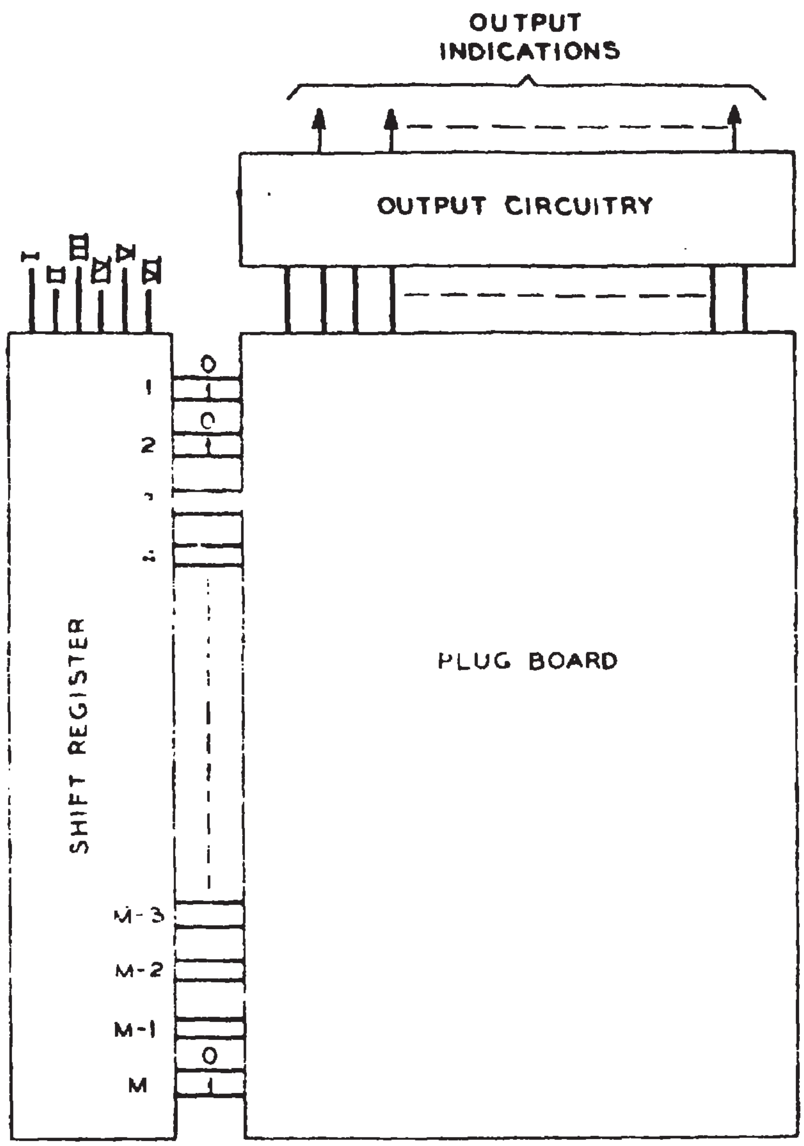
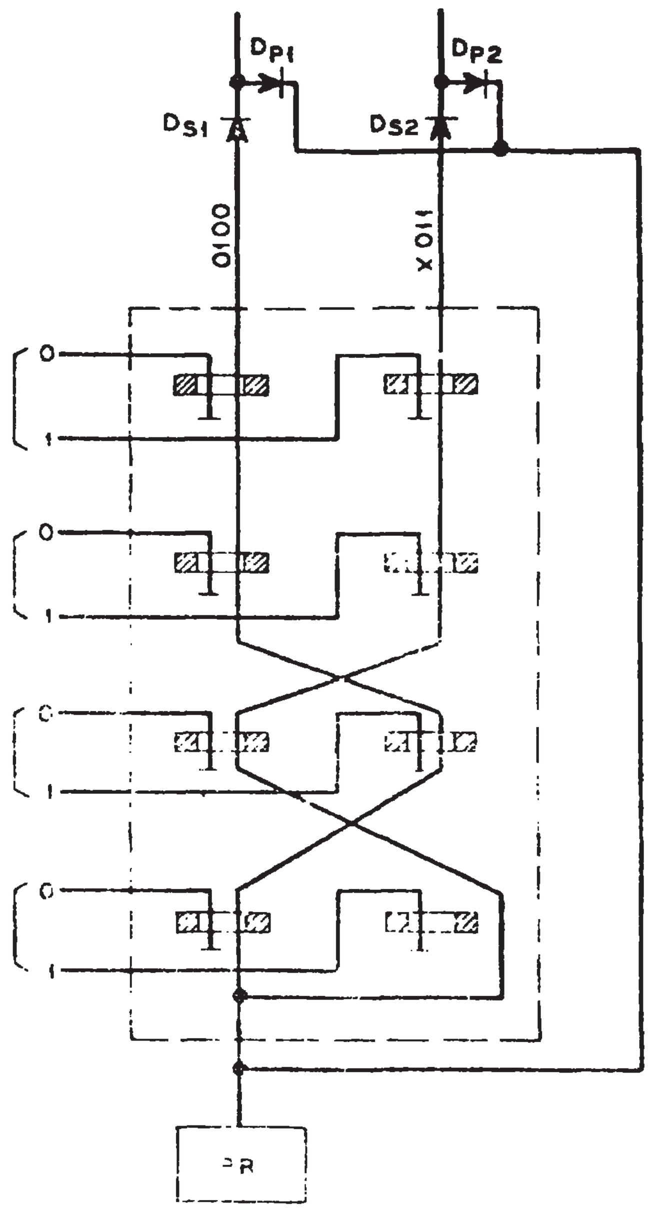


FIG.1

J.R. PIERCE
7-22-57



⊥ = GROUND

PARTS INSIDE OF DASHED LINE ARE PART OF PLUGBOARD

FIG. 2

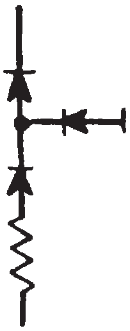


FIG. 3

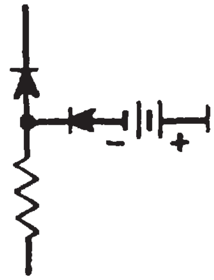
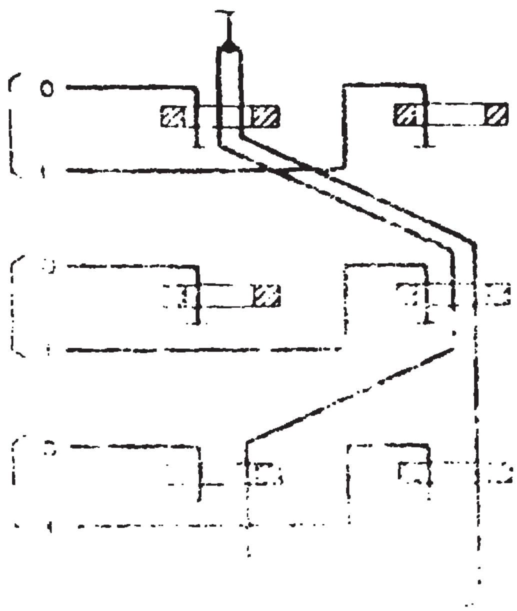
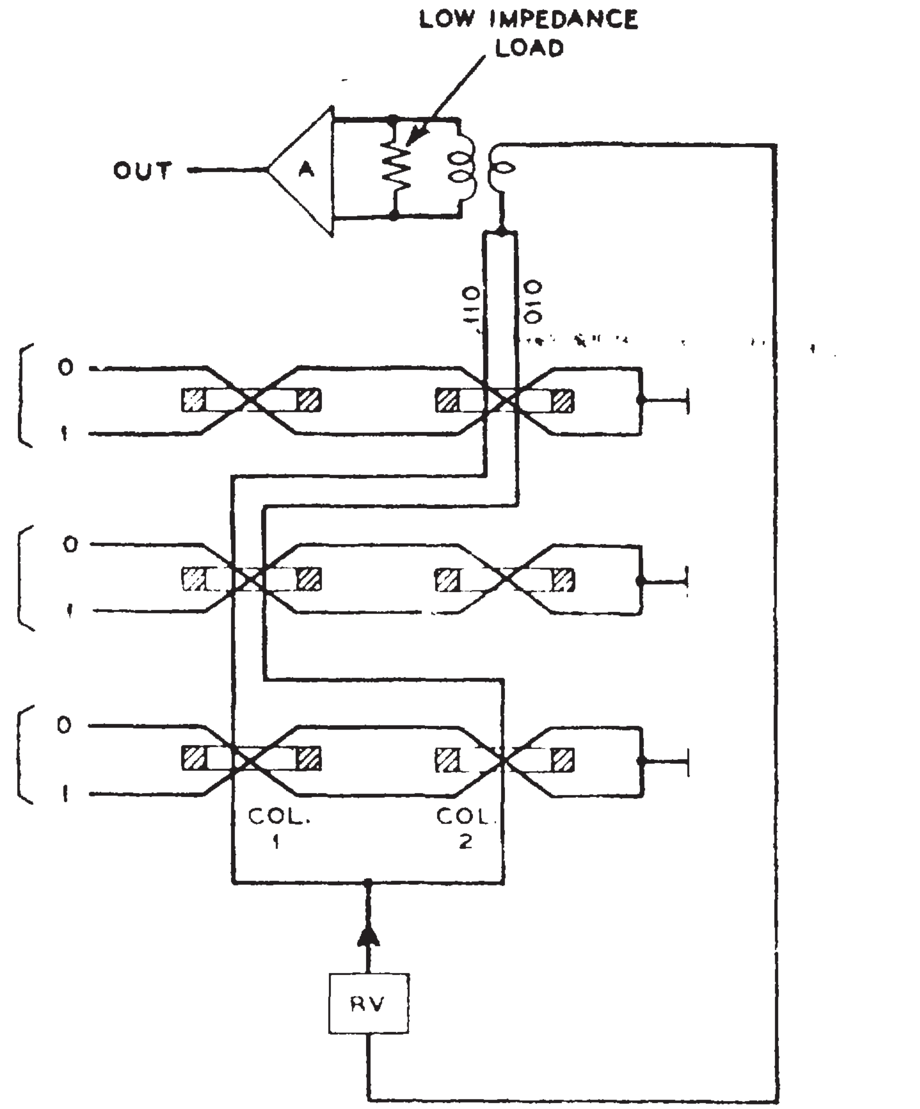


FIG. 4



J. R. PIERCE
7-22-57



⊥ = GROUND

FIG. 6

J. R. PIERCE
7-12-57

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

TECHNICAL ADJUNCT III

ESTIMATE OF TECHNICAL SITUATION IN CRYPTANALYSIS

It is very difficult for a non-specialist in the cryptographic field to provide a very penetrating appraisal of the technical position of the field. However, it seems important to say something in this regard, if only to emphasize the fact that the central difficulties are in fact technical and intellectual problems of a high order, and that management and engineering decisions which do not recognize this central fact are not likely to increase our actual proficiency in solving [redacted] Cryptanalysis, while it is more particularized than scientific research, has much of the exacting character of such research, particularly as this character is exhibited in research in mathematics and theoretical physics. It can be evaluated only by similar standards.

Cryptanalysis has always been a very specialized art based in part on a very high natural acumen in particular directions, and in part on very great experience. Before World War II it involved largely the diligent study of the relevant small numbers of messages, such as diplomatic messages, known or suspected to be of importance.

Since then many things have happened. One is the fact that cryptanalysis is now in a sense "big business." The COMINT effort in the more or less routine collection, transmission, and

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

processing of intercepted data is huge. It is clear that the management of such an enterprise has very little more to do with basic advances in cryptanalytic techniques than factory management has to do with basic physical research. As indicated elsewhere in this report, the two should be separated more sharply than they are at present, and a special systems-analysis attack on the goals of the routine production job should be mounted. This would provide for more efficient discharge of the production function and would provide the Agency with a stronger position in dealing with its customers. In addition, it would permit a better concentration of the existing most expert talent on the basic problems of cryptanalysis, and would provide a better foundation for a planning for systematic advances in the field.

Other changes in the field have involved a general increase in understanding of cryptanalysis and of practical ways of breaking into new ciphers, and the development of high-speed computers. It is clear that the high-speed computer is potentially a very powerful ally of the cryptanalyst. It permits him to undertake much more laborious tasks than he could do by hand and to explore more subtle facets of problems of cryptanalysis than was previously possible.

On the other hand, it appears that general advances in the field in other directions have favored the cryptographer as against the cryptanalyst. In general, the cryptanalyst relies on [redacted] for his victories. As this is more generally understood, the cryptographer is in a position to

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

provide systems which do not have these weaknesses or which are sufficiently complex to provide unreadable messages even if a certain number [redacted] Moreover, present cipher machines are largely mechanical. Their operations, however, are of a sort which lend themselves extremely well to the present electronic art. It should not be difficult with modern electronics to provide very compact machines with significantly more complex and flexible coding even than the present mechanical systems give.

It is the Panel's opinion that the advantages will be increasingly in favor of the cryptographer as against the cryptanalyst, in spite of the introduction of computer techniques. This may mean that machines are or will become so sophisticated that we can no longer hope to break [redacted] except on an accidental and irregular basis. The Panel's opinion in this matter is discussed elsewhere in the report. It is clear, however, that, without regard to one's actual prognosis, the stakes involved in the ability to read [redacted] even occasionally, are sufficiently great to induce us to make a strong effort to maximize our competence in the field. Moreover, it is only by the most intense effort toward the solution of current [redacted] that we can hope to keep into a position to read [redacted] as they, too, become more sophisticated.

The first element in such an effort is the establishment and maintenance of a nucleus of the most skillful possible analysts. It is important to notice that it is only the highest level of skill here that counts. Civil Service regulations, budgetary considerations, etc., should not be allowed to stand in the way of developing and conserving such skills. One is led to think of a deliberate concentration of the most skilled analysts in the Agency, combined with a close apprentice system, as a possible means of developing a larger body of cryptanalytic skill quickly.

The required skills and ability of a new generation of cryptanalysts may, however, be somewhat different from that of the old generation. An accompanying section speaks of the shift from low-order message and language structure to high-order structure as part of the problem of reading difficult codes. This is, broadly speaking, equivalent to a shift to a more abstract and general point of view. Whereas the traditional cryptanalyst could rely entirely on a particular "bag of tricks," the new expert must have more of the generality and abstractness of the typical professional scientist. He must, however, be just as sharp as the old generation was, and this is saying a great deal.

This evidently has some implications for the kinds of recruiting which the Agency should do. The Agency needs men of the same general sort as the best it has recruited previously, but they may require somewhat more formal scientific training. A particular illustration of the present situation is furnished by the apparent gap which exists in NSA between the traditional analysts and the skilled programmer on modern computing machines. New recruits should, among other requirements, be men who can bridge this gap.

The NSA initiated a promising research program several years ago, and it appears that this will pay increasing dividends in the future. The Panel believes, however, that the research program deserves some strengthening and reorienting. At present its most conspicuous achievement has been the establishment of a large-scale development program for new computer machines of types likely to be useful for the Agency. This somewhat hardware-centered program seems to give inadequate emphasis to the more subtle aspects of the Agency's problems.

For example, the Agency is probably more deeply interested in basic communication theory and in the complexities of linguistic structure and high-order language statistics than any other group in the country. This is a field of great subtlety and challenge, affording many opportunities for open and rewarding scientific advances. However, NSA appears to have no work going on in this or related information-theoretic directions.

The problem of recognition is also crucial. The use of visual displays as a possible means of recognizing and identifying obscure logical structures is described in another section. There is also a very important recognition problem involved in the [redacted] and other situations which seem particularly promising for exploitation.

Such very subtle questions deserve serious research over a period of years by a mixed team of mathematicians and statisticians, psychologists, and engineers. It would seem that the Agency should establish a strong effort in this field itself. In addition, it might well support such work at outside institutions, for example, Massachusetts Institute of Technology or Harvard.

Many of the problems of cryptanalysis are in effect mathematics, and a redoubled effort in this area seems also to be indicated. It is important, however, that the mathematical aspects be construed broadly and maintain a sufficient touch with cryptanalysis itself. The presence of security barriers, such as may exist for some of the members of part-time advisory groups to NSA such as SCAMP, the strong traditions of academic mathematics, etc., probably tend to shift the attention of many mathematicians to problems which fall within the normal intellectual organization of mathematics, but may have only peripheral or supporting interest to cryptanalysis.

If the Agency's research department is properly organized and administered its interests will span a broad and rewarding field of scientific endeavor of the highest level, and yet it should be perfectly clear that the core, purpose, and culmination of this effort is nothing more or less than the advance of the theory and practice of cryptanalysis.

TECHNICAL ANNEX IV

NSA SUPPORTED RESEARCH IN SOLID-STATE PHYSICS

The work sponsored by the NSA in solid-state physics may indeed be important academic research, but its relation to Agency needs is by no means up to the standards provided by their sponsored work in physics of the upper atmosphere and theoretical physics. This work appears to be an illustration of a common response to the frustrations that must enter when public support of fundamental research is intended to directly support so narrow a range of applications as NSA's needs provide. The scientific sponsors of such research recognize the difficulty, aggravated by security, of obtaining solid contributions to the large exploratory development program they are trying to support. In reaction, they support glamorous and widely acclaimed subjects and professors. The output from such work seems a justifiable object of public expenditure, and is usually hailed as scientific progress, although it has almost no interaction with the NSA. Such appears to be the case, for example, in the carefully chosen support of work on cyclotron resonance in metals at the University of California (where, interestingly enough, the discovery, attributed to NSA support, of this effect in tin followed its observation elsewhere in other metals, like bismuth, by a year or more). A similar situation apparently exists in support of the work at Harvard on the effects of pressure on electron spin resonance. This was noted as languishing because of the interest at Harvard in new spin oscillator effects. No unkindness is meant when it is said that perhaps professors, too, realize that at present the linkage of this research with the real interests of the supporting agency is too remote to take their first attention.

While the total annual cost of such work is less than half a million dollars, it seems important to bring out the missed opportunity to get done basic work really relevant to the needs of NSA. At the same time, of course, an alert basic development survey should make it possible to take advantage of the huge volume of fundamental physics of solids, and of other things, which is readily accessible for NSA purposes.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

HISTORY AND ORGANIZATION OF PANEL

(on Technology of Foreign Communications Intelligence)

A letter from the President on May 3, 1957, requested the formation of this Panel, for the technical study of [redacted] This followed recommendations of the President's Board of Consultants on Foreign Intelligence Activities, as approved by the President and referred to the Secretary of Defense and the Director, Office of Defense Mobilization, on January 29, 1957.

Such a panel was formed by the Science Advisory Committee, ODM, and has had a series of briefings by representatives of USCIB, including the following: CIA, FBI, NSA, NTPC, ODM, State Department, and other groups consuming COMINT output, such as National Indication Center, National Board of Estimates, etc., and a USAFSS group. The area of study was broadened to cover the whole range of communications intelligence and also ELINT, as seemed necessary to assess thoroughly the [redacted] problem. About 25 detailed sessions were coupled with numerous supplementary studies. Conferences among the Panel members numbered about 20. The Federal agencies were both friendly and cooperative in providing sensitive material. Most of the meetings were with NSA experts, whose willingness to meet the Panel's requests for highly specialized information was matched by their diligence in organizing and compacting it.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Several sub-groups in the Panel worked on special subjects, such as on [redacted] formulation of cryptanalytic problems, word recognizer schemes, etc. The Panel's judgments on the central issue of [redacted] ciphers had to be based on knowledge of the chance of getting information on coding machines and methods [redacted] Also, the relation of [redacted] activity to communications intelligence more generally came up repeatedly. Accordingly, the Panel has some special findings on technical activities in this field which may be available separately.

The crucial position of field work (interception and processing) in both the cost and effectiveness of the COMINT program caused the Panel to seek more information on this than could be reasonably gained in Washington. Hence, at a suitable time, which covered much of September 1957, Drs. Garwin and Selfridge visited important installations in the [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The Panel functioned in areas of Government more sensitive and restricted than most scientific people believe can be effectively studied. In this case, however, the cooperation and disclosures of the relevant agencies were mostly superb. For this, thanks are given to the Department of Defense, in particular, General G. B. Erskine; the NSA, in particular, Lieutenant General J. A. Samford; and to the Central Intelligence Agency and the Federal Bureau of Investigation.

Much more than permission, however, is necessary to give a satisfactory survey of complex communications intelligence technology. For the numerous briefings which objectively displayed the NSA work, Dr. A. Sinkov (with the full cognizance of Brigadier General W. M. Burgess), Mr. A. Levenson, Dr. S. Kullback, and their associates went to endless pains in completeness and clarity. They have our gratitude also for hospitable, but private, places where the Panel conferred, and studied highly secret material.

Indeed, the Panel could have handled such material, and worked out its own findings, only with the constant, skillful, and highly understanding support of the Office of Security Services, NSA. Its assignment of Mr. J. A. Grooms, Mr. A. [illegible]. Mathisen, and others to facilitate the whole project was essential to its progress.

Perspectives extending over the whole scope of modern American cryptology and communications intelligence were expertly and generously given the Panel by Lieutenant General Ralph Canine and Mr. William Friedman.

(b)(3)-P.L. 86-36

[redacted] and others of the Science Advisory Board of NSA kindly briefed us on their current considerations.

The Office of Defense Mobilization was headquarters, with Mr. D. Z. Beckler, of the Science Advisory Committee, making the whole study cogent and operable. We thank him and

Mr. Harold Lawrence also of the Executive Office of the President for devoted service to our cause.

L. W. Alvarez	University of California
H. W. Bode	Bell Telephone Laboratories, Inc.
R. L. Garwin	International Business Machines Corp.
D. A. Huffman	Mass. Institute of Technology
J. W. Milnor	Princeton University
J. R. Pierce	Bell Telephone Laboratories, Inc.
N. Rochester	International Business Machines Corp.
O. Selfridge	Lincoln Laboratories, MIT
J. W. Tukey, Consultant	Bell Telephone Laboratories, Inc. and Princeton University
W. O. Baker, Chairman	Bell Telephone Laboratories, Inc.
A. M. Gleason (part-time)	Harvard University

September 20, 1957